

53-1003226-01
19 March 2014



Network OS

Command Reference

Supporting Network OS v4.1.1

BROCADE

Copyright © 2013-2014 Brocade Communications Systems, Inc. All Rights Reserved.

Brocade, the B-wing symbol, Brocade Assurance, ADX, AnyIO, DCX, Fabric OS, FastIron, HyperEdge, ICX, MLX, MyBrocade, NetIron, OpenScript, VCS, VDX, and Vyatta are registered trademarks, and The Effortless Network and the On-Demand Data Center are trademarks of Brocade Communications Systems, Inc., in the United States and in other countries. Other brands and product names mentioned may be trademarks of others.

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. assume no liability or responsibility to any person or entity with respect to the accuracy of this document or any loss, cost, liability, or damages arising from the information contained herein 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
<i>Network OS Command Reference</i>	53-1002081-01	New document	December 2010
<i>Network OS Command Reference</i>	53-1002340-01	Updated for Network OS v2.1.0	September 2011
<i>Network OS Command Reference</i>	53-1002492-01	Updated for Network OS v2.1.1	December 2011
<i>Network OS Command Reference</i>	53-1002562-01	Updated for Network OS v3.0.0	September 2012
<i>Network OS Command Reference</i>	53-1002796-01	Updated for Network OS v3.0.1	December 2012
<i>Network OS Command Reference</i>	53-1002796-02	Updated for Network OS v3.0.1a	March 2013
<i>Network OS Command Reference</i>	53-1002796-04	Updated for Network OS v3.0.1b	July 2013
<i>Network OS Command Reference</i>	53-1002841-01	Updated for Network OS v4.0.0	July 2013
<i>Network OS Command Reference</i>	53-1003115-01	Updated for Network OS v4.1.0	February 2014
<i>Network OS Command Reference</i>	53-1003226-01	Updated for Network OS v4.1.1	March 2014

Contents

About This Document

How this document is organized	xxxiii
Supported hardware and software	xxxiii
What's new in this document.	xxxiv
Document conventions.	xxxiv
Text formatting	xxxiv
Command syntax conventions	xxxv
Notes, cautions, and warnings	xxxvi
Key terms	xxxvi
Notice to the reader	xxxvii
Additional information.	xxxvii
Brocade resources.	xxxvii
Other industry resources.	xxxvii
Getting technical help.	xxxviii
Document feedback	xxxviii

Chapter 1

Using the Network OS CLI

DCB command line interface	1
Saving your configuration changes	1
Network OS CLI RBAC permissions	2
Default roles	2
Accessing the Network OS CLI through Telnet	2
Network OS CLI command modes	3
Network OS CLI keyboard shortcuts	8
Using the do command as a shortcut	8
Displaying Network OS CLI commands and command syntax.	9
Network OS CLI command completion	10
Network OS CLI command output modifiers.	10
Show command output information	11

Chapter 2

Network OS Commands

aaa accounting.	13
aaa authentication.	15
access-group	17

access-list	18
activate (NSX Controller connection profile)	19
activate (VXLAN gateway)	20
address-family ipv4 unicast (BGP)	21
address-family ipv4 unicast (VRF)	22
advertise dcbx-fcoe-app-tlv	23
advertise dcbx-fcoe-logical-link-tlv	24
advertise dcbx-iscsi-app-tlv	25
advertise dcbx-tlv	26
advertise dot1-tlv	27
advertise dot3-tlv	28
advertise optional-tlv	29
advertise-backup	30
advertisement interval (fabric-map)	31
advertisement-interval (VRRP)	32
ag	33
ag enable	34
aggregate-address (BGP)	35
alias	36
alias-config	37
allow non-profiled-macs	38
always-compare-med (BGP)	39
always-propagate (BGP)	40
area nssa (OSPF)	41
area range (OSPF)	42
area stub (OSPF)	43
area virtual-link (OSPF)	44
arp	46
as-path-ignore (BGP)	47
attach rbridge-id	48
attach vlan	49
auto-cost reference-bandwidth (OSPF)	50
backup-advertisement-interval	51
banner incoming	52
banner login	53
banner motd	55
bgp-redistribute-internal (BGP)	56
bind	57
bpdu-drop enable	58
bridge-priority	59
capability as4 (BGP)	60
capture packet interface	61
cbs	63
cee	64
cee-map (configuration)	65

cee-map (FCoE)	66
certutil import ldapca	67
certutil import sshkey	69
certutil import syslogca	71
channel-group	73
chassis beacon	75
chassis disable	76
chassis enable	77
chassis fan airflow-direction	78
chassis virtual-ip virtual-ipv6	79
cidrecov	80
cipherset	83
cisco-interoperability	84
class	85
class-map	87
clear arp	88
clear counters	90
clear counters access-list	92
clear counters access-list (interface)	94
clear counters access-list (ip)	96
clear counters access-list (MAC)	98
clear counters interface	100
clear counters slot-id	102
clear counters (IP)	103
clear counters (MAC)	105
clear counters storm-control	107
clear dot1x statistics	109
clear dot1x statistics interface	110
clear edge-loop-detection	111
clear fcoe login	113
clear ip bgp dampening	114
clear ip bgp flap-statistics	115
clear ip bgp local routes	116
clear ip bgp neighbor	117
clear ip bgp routes	118
clear ip bgp traffic	119
clear ip dhcp relay statistics	120
clear ip igmp groups	121
clear ip igmp statistics interface	123
clear ip ospf	125
clear ip pim mcache	127
clear ip pim rp-map	128
clear ip pim traffic	129
clear ip route	130
clear lacp	131

clear lacp counters	132
clear lldp neighbors	133
clear lldp statistics	134
clear logging auditlog	135
clear logging raslog	136
clear mac-address-table dynamic	137
clear nas statistics	139
clear overlay-gateway	140
clear policy-map-counters	141
clear sessions	142
clear sflow statistics	143
clear spanning-tree counter	144
clear spanning-tree detected-protocols	145
clear support	146
clear udd statistics	147
clear vrrp statistics	148
client-to-client-reflection (BGP)	150
clock set	151
clock timezone	152
cluster-id (BGP)	154
compare-med-empty-aspath (BGP)	155
compare-routerid (BGP)	156
configure terminal	157
conform-set-dscp	158
conform-set-prec	159
conform-set-tc	160
connector	161
continue	162
copy	163
copy default-config startup-config	165
copy running-config startup-config	166
copy snapshot (logical chassis cluster mode)	167
copy support	168
copy support-interactive	170
cos-mutation	171
cos-traffic-class	172
counter reliability	173
dampening (BGP)	174
database-overflow-interval (OSPF)	175
debug access-list-log buffer	176
debug dhcp packet buffer	177
debug dhcp packet buffer clear	178
debug dhcp packet buffer interface	179
debug fcoe show swcfg	181
debug ip	182

debug ip bgp.....	184
debug ip bgp address-family ipv4 unicast.....	185
debug ip bgp neighbor.....	186
debug ip igmp.....	187
debug ip ospf.....	189
debug ip pim.....	190
debug ip rtm.....	191
debug ip vrf.....	193
debug lacp.....	194
debug lldp dump.....	196
debug lldp packet.....	198
debug lldp dump.....	200
debug spanning-tree.....	201
debug udd.....	203
debug vrrp.....	204
default-information-originate (BGP).....	206
default-information-originate (OSPF).....	207
default-local-preference (BGP).....	208
default-metric (BGP).....	209
default-metric (OSPF).....	210
default-passive-interface (OSPF).....	211
delete.....	212
deny (extended ACLs).....	213
deny (standard ACLs).....	215
description (interfaces).....	216
description (LLDP).....	217
description (Port Mirroring).....	218
description (VRRP).....	219
desire-distance.....	220
dhcp auto-deployment enable.....	221
diag burninerrclear.....	222
diag clearerror.....	223
diag portledtest.....	224
diag portloopbacktest.....	226
diag post enable.....	228
diag prbstest.....	229
diag setcycle.....	230
diag systemverification.....	232
diag turboramtest.....	233
dir.....	234
distance (BGP).....	235
distance (OSPF).....	236
distribute-list route-map (OSPF).....	237
dot1x authentication.....	238
dot1x enable.....	239

dot1x port-control	240
dot1x quiet-period	241
dot1x reauthenticate interface	242
dot1x reauthentication	243
dot1x reauthMax	244
dot1x test eapol-capable	245
dot1x test timeout	246
dot1x timeout re-authperiod	247
dot1x timeout server-timeout	248
dot1x timeout supp-timeout	249
dot1x timeout tx-period	250
dpod	251
dscp-cos	252
dscp-mutation	253
dscp-traffic-class	254
ebs	255
eir	256
hello-interval (ELD)	257
edge-loop-detection port-priority	258
edge-loop-detection vlan	259
enable statistics direction	260
end	261
enable statistics direction	262
enable	263
enforce-first-as (BGP)	264
enodes-config	265
error-disable-timeout enable	266
error-disable-timeout interval	267
exceed-set-dscp	268
exceed-set-prec	269
exceed-set-tc	270
exit	271
external-lsdb-limit (OSPF)	272
fabric ecmp load-balance	273
fabric ecmp load-balance-hash-swap	274
fabric isl enable	275
fabric neighbor-discovery disable	276
fabric route mcast	277
fabric trunk enable	278
fabric vlag	279
fabric-map	280
fast-external-failover (BGP)	281
fastboot	282
fcmap	283
fcoe	284

fcoe-enodes	285
fcoe-profile (AMPP)	286
fcoeport	287
fcsp auth.....	288
fcsp auth-secret dhchap	290
fill-word	291
filter-change-update-delay.....	292
fips root disable	293
fips selftests.....	294
fips zeroize	295
firmware activate	296
firmware commit	298
firmware download	299
firmware download ftp.....	302
firmware download interactive	304
firmware download logical-chassis.....	305
firmware download scp	307
firmware download sftp.....	309
firmware download usb.....	311
firmware install.....	313
firmware recover	315
firmware restore.....	316
firmware sync.....	317
forward-delay	318
ha chassisreboot	319
ha disable.....	320
ha enable	321
ha failover.....	322
ha sync start.....	323
ha sync stop	324
hardware.....	325
hello (LLDP)	326
hello (UDLD).....	327
hello-interval.....	328
hello-time	329
hello-timer.....	330
hold-time.....	331
http server shutdown.....	332
inactivity-timer	333
install-igp-cost (BGP)	334
instance	335
interface	336
interface (range specification)	338
interface loopback.....	342
interface management	343

interface ve	345
interface vlan	346
ip access-group	348
ip access-list	349
ip address	351
ip address (NSX controller configuration)	352
ip arp-aging-timeout	353
ip as-path access-list	354
ip community-list extended	355
ip community-list standard	356
ip dhcp relay address	357
ip directed-broadcast	358
ip dns	359
ip echo-reply	360
ipv6 echo-reply	361
ip http-server enable	362
ip icmp rate-limit	363
ipv6 icmp rate-limit	364
ip igmp immediate-leave	365
ip igmp last-member-query-interval	366
ip igmp query-interval	367
ip igmp query-max-response-time	368
ip igmp snooping enable (global version)	369
ip igmp snooping enable	370
ip igmp snooping fast-leave	371
ip igmp snooping mrouter	372
ip igmp snooping mrouter-timeout	374
ip igmp snooping querier enable	375
ip igmp static-group	376
ip interface	377
ip load-sharing	379
ip mtu	380
ip multicast-boundary	381
ip ospf active	382
ip ospf passive	383
ip ospf area	384
ip ospf auth-change-wait-time	385
ip ospf authentication-key	386
ip ospf cost	387
ip ospf database-filter	388
ip ospf dead-interval	390
ip ospf hello-interval	391
ip ospf md5-authentication	392
ip ospf mtu-ignore	394
ip ospf network	395

ip ospf passive	396
ip ospf priority	397
ip ospf retransmit-interval	398
ip ospf transmit-delay	399
ip pim dr-priority	400
ip pim-sparse	401
ip policy route-map	402
ip prefix-list	403
ip proxy-arp	404
ip route	405
ip route next-hop ospf	407
ip route next-hop-enable-default	408
ip route next-hop-recursion	409
ip route next-hop-vrf	410
ip router-id	411
ip unreachable	412
ipv6 echo-reply	413
ipv6 icmp rate-limit	414
ipv6 ra-guard	415
ipv6 route	416
ipv6 unreachable	417
iscsi-priority	418
isl-r_rdy	419
keep-alive timeout (fabric-map)	420
l2traceroute	421
lACP default-up	423
lACP port-priority	424
lACP system-priority	425
lACP timeout	426
ldap-server host	427
ldap-server maprole	429
license add	430
license remove	431
line vty exec-timeout	432
linecard	433
lldp dcbx-version	435
lldp disable	436
lldp iscsi-priority	437
lldp profile	438
load-balance	439
local-as (BGP)	440
log-dampening-debug (BGP)	441
logging auditlog class	442
logging raslog console	443
logging syslog-facility local	444

logging syslog-server	445
logical-chassis principal-priority	446
logical-chassis principal-switchover	447
long-distance	448
long-distance-isl	450
mac	452
mac access-group	453
mac access-list extended	454
mac access-list standard	455
mac-address-reduction	456
mac-address-table	457
mac-group	459
mac-rebalance	460
management	461
map	462
map fport interface fcoe	463
map qos	464
map sflow	465
match	466
match (route map)	467
match access-list	469
match as-path	470
match community	471
match interface	472
match ip address	473
match ip next-hop	474
match metric	475
match protocol bgp	476
match route-type	477
match tag	478
max-age	479
max-hops	480
max-mcache	481
max-metric router-lsa (OSPF)	482
max-route	484
maxas-limit (BGP)	485
maximum-paths (BGP)	486
maximum-paths ebgp ibgp (BGP)	487
med-missing-as-worst (BGP)	488
message-interval	489
metric-type (OSPF)	490
minimum-links	491
mode	492
mode (27x40 GbE line card)	493
modes	494

monitor session	495
monitor-session (VXLAN gateway).....	496
mtu	498
multipath (BGP)	499
multiplier (LLDP)	500
multiplier (UDLD)	501
nas auto-qos.....	502
nas server-ip.....	503
nbr-timeout.....	504
neighbor (BGP).....	505
neighbor (OSPF).....	507
neighbor advertisement-interval (BGP)	508
neighbor as-override (BGP)	509
neighbor capability as4 (BGP)	510
neighbor default-originate (BGP).....	511
neighbor description (BGP)	512
neighbor ebgp-multihop (BGP)	513
neighbor enforce-first-as (BGP).....	514
neighbor filter-list (BGP)	515
neighbor local-as (BGP)	516
neighbor maxas-limit in (BGP).....	517
neighbor maximum-prefix (BGP).....	518
neighbor next-hop-self (BGP)	519
neighbor password (BGP)	520
neighbor peer-group (BGP)	521
neighbor prefix-list (BGP).....	522
neighbor remote-as (BGP).....	523
neighbor remove-private-as (BGP)	524
neighbor route-map (BGP).....	525
neighbor route-reflector-client (BGP)	526
neighbor send-community (BGP)	527
neighbor shutdown (BGP)	528
neighbor soft-reconfiguration inbound (BGP)	529
neighbor timers (BGP)	530
neighbor unsuppress-map (BGP)	531
neighbor update-source (BGP)	532
neighbor weight (BGP).....	534
network (BGP)	535
next-hop-enable-default (BGP)	536
next-hop-recursion (BGP).....	537
nport	538
nport interface Fibrechannel	539
nssa-translator (OSPF).....	540
nsx-controller client-cert	541
nsx-controller name.....	542

nsx-controller name reconnect	543
ntp authentication-key	544
ntp server	545
oscmd	546
overlay-gateway (for VXLAN)	548
password-attributes	549
password-attributes admin-lockout enable	551
pdu-rx-limit	552
permit (extended ACLs)	553
permit (standard ACLs)	555
pg	556
ping	557
police cir	559
police-priority-map	560
policy-map	561
port-channel path-cost	562
port-group	563
port-profile (global configuration mode).	564
port-profile (port-profile-domain configuration mode).	565
port-profile-domain	566
port-profile-port	567
port-shape	569
power-off	570
power-off linecard	571
power-on	572
power-on linecard	573
precedence	574
preempt-mode	575
priority	576
priority-group-table	577
priority-tag	579
private-vlan	580
private-vlan association	581
profile	582
prom-access disable	583
protect-mode enable	584
protocol edge-loop-detection	585
protocol lldp	586
protocol spanning-tree	587
protocol udd	588
protocol vrrp	589
protocol vrrp-extended	590
pwd	591
qos cos	592
qos cos-mutation	593

qos cos-traffic-class	594
qos dscp-cos	595
qos dscp-mutation	596
qos dscp-traffic-class	597
qos flowcontrol tx rx	598
qos flowcontrol pfc	599
qos map cos-mutation	600
qos map cos-traffic-class	601
qos map dscp-cos	602
qos map dscp-mutation	603
qos map dscp-traffic-class	605
qos red profile	606
qos trust cos	607
qos trust dscp	608
qos queue multicast scheduler	609
qos queue scheduler	611
qos random-detect cos	613
qos rcv-queue cos-threshold	614
qos rcv-queue multicast rate-limit	616
qos rcv-queue multicast threshold	617
qos-profile (AMPP)	619
radius-server	620
rasman	622
rate-limit-delay get netconf	625
rate-limit-delay set netconf	626
rbridge-id	627
rd (route distinguisher)	629
reconnect-interval	630
redistribute (BGP)	631
redistribute (OSPF)	632
region	633
reload	634
remap fabric-priority	636
remap lossless-priority	637
rename	638
rename (Access Gateway mode)	639
resequence access-list	640
reserved-vlan	641
restrict-flooding	642
revision	643
rfc1583-compatibility (OSPF)	644
rfc1587-compatibility (OSPF)	645
rib-route-limit (BGP)	646
rmon alarm	647
rmon collection history	648

rmon collection stats	649
rmon event	650
role name	651
route-map	652
router bgp	654
router ospf	655
router pim	656
route-target	657
rp-address	658
rspan-vlan	659
rule	660
scheduler	661
secpolicy activate	662
secpolicy defined-policy	663
security-profile (AMPP)	665
seq (extended IP ACLs)	666
seq (standard IP ACLs)	669
seq (extended MAC ACLs)	670
seq (standard MAC ACLs)	672
service password-encryption	673
service-policy	674
set as-path	675
set as-path prepend	676
set automatic-tag	678
set comm-list	679
set community	680
set cos traffic-class	681
set dscp	682
set dampening	683
set distance	684
set ip interface null0	685
set ip next-hop	686
set local-preference	687
set metric	688
set metric-type	689
set origin	690
set-priority	691
set route-type	692
set tag	693
set weight	694
sflow collector	695
sflow enable (global version)	696
sflow enable (interface version)	697
sflow polling-interval (global version)	698
sflow polling-interval (interface version)	699

sflow sample-rate (global version)	700
sflow sample-rate (interface version)	701
sflow-profile	702
sfp breakout	703
short-path-forwarding	704
show access-list	705
show access-list interface	706
show access-list ip	707
show access-list mac	708
show access-list-log buffer	709
show ag	710
show ag map	712
show ag pg	714
show arp	715
show bpdu-drop	717
show capture packet interface	718
show cee maps	719
show cert-util ldapca	720
show cert-util sshkey	721
show cert-util syslogca	722
show chassis	723
show cipherset	727
show class-maps	728
show cli	729
show cli history	730
show clock	731
show config snapshot	732
show copy-support status	733
show dadstatus	734
show debug dhcp packet	735
show debug dhcp packet buffer	736
show debug ip bgp all	738
show debug ip igmp	739
show debug ip pim	740
show debug lacp	741
show debug lldp	742
show debug spanning-tree	743
show debug udd	744
show debug vrrp	745
show defaults threshold	746
show default-vlan	748
show dpod	749
show diag burninerrshow	751
show diag burninerrshowerrLog	752
show diag burninstatus	754

show diag post results	755
show diag setcycle	757
show diag status	758
show dot1x	759
show dot1x all	760
show dot1x diagnostics interface	761
show dot1x interface	762
show dot1x session-info interface	763
show dot1x statistics interface	764
show dpod	765
show edge-loop-detection detail	766
show edge-loop-detection globals	767
show edge-loop-detection interface	768
show edge-loop-detection rbridge-id	770
show environment fan	771
show environment history	772
show environment power	774
show environment sensor	775
show environment temp	776
show fabric all	777
show fabric ecmp load-balance	778
show fabric isl	779
show fabric islports	783
show fabric port-channel	787
show fabric route linkinfo	788
show fabric route multicast	792
show fabric route neighbor-state	795
show fabric route pathinfo	798
show fabric route topology	806
show fabric trunk	809
show fcoe fabric-map	812
show fcoe interface	814
show fcoe login	815
show fcoe map	816
show fcsp auth-secret dh-chap	817
show fibrechannel login	818
show file	820
show fips	821
show firmwaredownloadhistory	822
show firmwaredownloadstatus	823
show global-running-config	825
show ha	827
show history	829
show interface	830
show interface description	834

show interface FibreChannel	835
show interface management	841
show interface stats	843
show interface status	845
show interface trunk	846
show inventory	847
show ip bgp	849
show ip bgp attribute-entries	850
show ip bgp dampened-paths	851
show ip bgp filtered-routes	852
show ip bgp flap-statistics	853
show ip bgp neighbor	854
show ip bgp neighbors	855
show ip bgp neighbors advertised-routes	856
show ip bgp neighbors flap-statistics	857
show ip bgp neighbors received	858
show ip bgp neighbors received-routes	859
show ip bgp neighbors routes	860
show ip bgp neighbors routes-summary	861
show ip bgp peer-group	862
show ip bgp routes	863
show ip bgp routes age	864
show ip bgp routes as-path-access-list	865
show ip bgp routes community	866
show ip bgp routes community-access-list	867
show ip bgp routes community-reg-expression	868
show ip bgp routes longer-prefixes	869
show ip bgp routes neighbor nexthop local unreachable ...	870
show ip bgp routes prefix-list regular-expression route-map	871
show ip bgp routes summary detail	872
show ip dhcp relay address interface	873
show ip dhcp relay address rbridge-id	875
show ip dhcp relay statistics	877
show ip igmp groups	879
show ip igmp interface	882
show ip igmp snooping	884
show ip igmp statistics	885
show ip interface	887
show ip interface loopback	890
show ip interface ve	891
show ip ospf	892
show ip ospf area	893
show ip ospf border-routers	895
show ip ospf config	896
show ip ospf database	897

show ip ospf interface	900
show ip ospf neighbor	902
show ip ospf redistribute route	904
show ip ospf routes	905
show ip ospf summary.	906
show ip ospf traffic	907
show ip ospf virtual	909
show ip pim bsr	910
show ip pim group	911
show ip pim mcache	912
show ip pim neighbor.	913
show ip pim rpf.	914
show ip pim rp-hash.	915
show ip pim rp-map	916
show ip pim rp-set	917
show ip pim-sparse	918
show ip pim traffic	920
show ip route	921
show ipv6 route	924
show lacp	925
show lacp sys-id	926
show license.	927
show license id.	929
show linecard	930
show lldp interface.	932
show lldp neighbors.	933
show lldp statistics.	935
show logging auditlog	936
show logging raslog	937
show mac-address-table	939
show media	942
show media interface	943
show media linecard	946
show mm	948
show monitor	949
show name-server brief.	950
show name-server detail	951
show name-server nodefind	953
show name-server zonemember	954
show nas statistics.	956
show netconf client-capabilities	957
show netconf-state capabilities	958
show netconf-state datastores	959
show netconf-state schemas	960
show netconf-state sessions.	961

show netconf-state statistics	962
show notification stream	963
show nsx controller	964
show ntp status	966
show overlapping-vlan-resource usage	967
show overlay-gateway	968
show policymap	970
show port port-channel	972
show port-channel	973
show port-profile	974
show port-profile domain	975
show port-profile interface	976
show port-profile name	977
show port-security	978
show port-security addresses	979
show port-security interface	980
show port-security oui interface	982
show port-security sticky interface	983
show process cpu	984
show process info	985
show process memory	986
show prom-access	987
show qos flowcontrol interface	988
show qos interface	990
show qos maps	992
show qos maps dscp-cos	993
show qos maps dscp-mutation	994
show qos maps dscp-traffic-class	995
show qos queue interface	996
show qos rcv-queue interface	997
show qos rcv-queue multicast	998
show qos red profiles	999
show qos red statistics interface	1001
show rbridge-id	1002
show rbridge-running config	1003
show rbridge-local-running-config	1007
show redundancy	1010
show rmon	1011
show rmon history	1013
show route-map	1014
show route-map interface	1016
show running reserved-vlan	1018
show running-config	1019
show running-config aaa	1020
show running-config aaa accounting	1021

show running-config access-list	1022
show running-config ag	1023
show running-config banner	1025
show running-config cee-map	1026
show running-config class-map	1027
show running-config diag post	1028
show running-config dot1x	1029
show running-config dpod	1030
show running-config fabric route mcast	1031
show running-config fcoe	1032
show running-config fcsp auth	1033
show running-config hardware connector	1034
show running-config interface fcoe	1035
show running-config interface FibreChannel	1036
show running-config interface fortygigabitethernet	1038
show running-config interface fortygigabitethernet bpdu-drop	1039
show running-config interface fortygigabitethernet cee ...	1040
show running-config interface fortygigabitethernet channel-group	1041
show running-config interface fortygigabitethernet description	1042
show running-config interface fortygigabitethernet dot1x .	1043
show running-config interface fortygigabitethernet fabric .	1045
show running-config interface fortygigabitethernet fcoeport	1046
show running-config interface fortygigabitethernet lacp. ...	1047
show running-config interface fortygigabitethernet lldp ...	1048
show running-config interface fortygigabitethernet mac ..	1049
show running-config interface fortygigabitethernet mtu ...	1050
show running-config interface fortygigabitethernet port-profile-port	1051
show running-config interface fortygigabitethernet priority-tag	1052
show running-config interface fortygigabitethernet qos ...	1053
show running-config interface fortygigabitethernet rmon. .	1054
show running-config interface fortygigabitethernet sflow. .	1055
show running-config interface fortygigabitethernet shutdown	1056
show running-config interface fortygigabitethernet switchport	1057
show running-config interface fortygigabitethernet udld ..	1058
show running-config interface fortygigabitethernet vlan. ...	1059
show running-config interface gigabitethernet	1060
show running-config interface gigabitethernet bpdu-drop .	1061
show running-config interface gigabitethernet channel-group	1062

show running-config interface gigabitethernet description	1063
show running-config interface gigabitethernet dot1x	1064
show running-config interface gigabitethernet lacp	1066
show running-config interface gigabitethernet lldp	1067
show running-config interface gigabitethernet mac	1068
show running-config interface gigabitethernet mtu	1069
show running-config interface gigabitethernet port-profile-port	1070
show running-config interface gigabitethernet priority-tag . .	1071
show running-config interface gigabitethernet qos	1072
show running-config interface gigabitethernet rmon	1073
show running-config interface gigabitethernet sflow	1074
show running-config interface gigabitethernet shutdown. .	1075
show running-config interface gigabitethernet switchport . .	1076
show running-config interface gigabitethernet udld	1077
show running-config interface gigabitethernet vlan	1078
show running-config interface management	1079
show running-config interface port-channel	1080
show running-config interface tengigabitethernet.	1081
show running-config interface tengigabitethernet bpdu-drop	1082
show running-config interface tengigabitethernet cee	1083
show running-config interface tengigabitethernet channel-group	1084
show running-config interface tengigabitethernet description	1085
show running-config interface tengigabitethernet dot1x . .	1086
show running-config interface tengigabitethernet fabric . .	1088
show running-config interface tengigabitethernet fcport	1089
show running-config interface tengigabitethernet lacp. . .	1090
show running-config interface tengigabitethernet lldp . . .	1091
show running-config interface tengigabitethernet mac. . .	1092
show running-config interface tengigabitethernet mtu. . .	1093
show running-config interface tengigabitethernet port-profile-port	1094
show running-config interface tengigabitethernet priority-tag	1095
show running-config interface tengigabitethernet qos	1096
show running-config interface tengigabitethernet rmon. . .	1097
show running-config interface tengigabitethernet sflow. . .	1098
show running-config interface tengigabitethernet shutdown	1099
show running-config interface tengigabitethernet switchport.	1100
show running-config interface tengigabitethernet udld . . .	1101
show running-config interface tengigabitethernet vlan. . .	1102

show running-config interface vlan	1103
show running-config interface vlan ip	1104
show running-config ip access-list	1106
show running-config ip dns	1107
show running-config ip igmp	1108
show running-config ip route	1109
show running-config ldap-server	1110
show running-config line	1111
show running-config logging	1112
show running-config logging auditlog class	1113
show running-config logging raslog	1114
show running-config logging syslog-facility	1115
show running-config logging syslog-server	1116
show running-config mac-address-table	1117
show running-config monitor	1118
show running-config ntp	1119
show running-config password-attributes	1120
show running-config police-priority-map	1121
show running-config policy-map	1122
show running-config port-profile	1123
show running-config port-profile activate	1124
show running-config port-profile fcoe-profile	1125
show running-config port-profile qos-profile	1126
show running-config port-profile security-profile	1127
show running-config port-profile static	1128
show running-config port-profile vlan-profile	1129
show running-config port-profile-domain	1131
show running-config protocol cdp	1132
show running-config protocol edge	1133
show running-config protocol lldp	1134
show running-config protocol spanning-tree mstp	1135
show running-config protocol spanning-tree pvst	1136
show running-config protocol spanning-tree rpvt	1137
show running-config protocol spanning-tree rstp	1138
show running-config protocol spanning-tree stp	1139
show running-config protocol udld	1140
show running-config radius-server	1141
show running-config rbridge-id	1142
show running-config rbridge-id linecard	1143
show running-config rbridge-id ssh	1144
show running-config rmon	1145
show running-config role	1146
show running-config route-map	1147
show running-config rule	1148
show running-config secpolicy	1150

show running-config sflow	1152
show running-config sflow-policy	1153
show running-config sflow-profile	1154
show running-config snmp-server	1155
show running-config snmp-server engineid	1156
show running-config ssh	1157
show running-config ssh server	1158
show running-config ssh server key-exchange	1160
show running-config support	1161
show running-config support autoupload-param	1162
show running-config switch-attributes	1163
show running-config system-monitor	1164
show running-config system-monitor-mail	1165
show running-config tacacs-server	1166
show running-config telnet server	1167
show running-config threshold-monitor	1168
show running-config threshold-monitor interface	1169
show running-config threshold-monitor security	1170
show running-config threshold-monitor sfp	1171
show running-config username	1172
show running-config vcs	1173
show running-config zoning	1174
show running-config zoning defined-configuration	1175
show running-config zoning enabled-configuration	1177
show running-config nas server-ip	1179
show secpolicy	1180
show sflow	1181
show sflow-profile	1183
show sfm	1184
show sfp	1186
show slots	1187
show span path	1189
show spanning-tree	1190
show spanning-tree brief	1191
show spanning-tree interface	1193
show spanning-tree mst brief	1195
show spanning-tree mst detail	1196
show spanning-tree mst instance	1199
show spanning-tree mst interface	1201
show ssh server status	1203
show ssh server rekey-interval status	1204
show startup-config	1205
show startup-db	1206
show statistics access-list	1207
show statistics access-list interface	1209

show storm-control	1210
show support	1212
show system	1213
show system internal nas	1214
show system monitor	1215
show telnet server status	1216
show threshold monitor	1217
show tunnel	1218
show udd	1220
show udd interface	1221
show udd statistics	1223
show users	1224
show vcs	1225
show version	1228
show virtual-fabric status	1230
show vlan	1231
show vlan classifier	1234
show vlan private-vlan	1235
show vlan rspan-vlan	1236
show vnetwork	1237
show vrf	1240
show vrrp	1241
show zoning enabled-configuration	1243
show zoning operation-info	1244
shutdown	1245
shutdown (UDLD)	1246
shutdown (STP)	1247
shutdown-time	1248
slot	1249
snmp-server community	1250
snmp-server contact	1251
snmp-server context	1252
snmp-server engineid local	1253
snmp-server host	1254
snmp-server location	1256
snmp-server sys-descr	1257
snmp-server user	1258
snmp-server v3host	1260
source	1261
spanning-tree autoedge	1263
spanning-tree bpdu-mac	1264
spanning-tree cost	1265
spanning-tree edgeport	1266
spanning-tree guard root	1267
spanning-tree hello-time	1268

spanning-tree instance	1269
spanning-tree link-type	1270
spanning-tree portfast	1271
spanning-tree priority	1272
spanning-tree restricted-role	1273
spanning-tree restricted-tcn	1274
spanning-tree shutdown	1275
spanning-tree vlan	1276
speed (Ethernet)	1277
speed (Fibre Channel)	1278
speed (LAG)	1279
speed (port-channel)	1280
spt-threshold	1281
ssh	1282
ssh server key-exchange dh-group-14	1284
ssh server rekey-interval	1285
ssh server shutdown	1286
ssh server status	1287
static-network (BGP)	1288
storm-control ingress	1289
summary-address	1291
support	1292
support autoupload enable	1293
support autoupload-param	1294
switch-attributes	1295
switchport	1296
switchport access	1297
switchport mode	1299
switchport mode private-vlan	1300
switchport mode trunk-no-default-native	1302
switchport port-security	1304
switchport port-security mac-address	1305
switchport port-security max	1306
switchport port-security oui	1307
switchport port-security shutdown-time	1308
switchport port-security sticky	1309
switchport port-security violation	1310
switchport private-vlan association trunk	1311
switchport private-vlan host-association	1312
switchport private-vlan mapping	1313
switchport private-vlan trunk allowed vlan	1314
switchport private-vlan trunk native-vlan	1316
switchport trunk allowed vlan rspan-vlan	1317
switchport trunk default-vlan	1319
switchport trunk native-vlan	1320

switchport trunk native-vlan-untagged	1322
switchport trunk native-vlan-xtagged	1323
switchport trunk tag native-vlan	1325
system-description	1326
system-max	1327
system-monitor	1328
system-monitor-mail	1330
system-name	1332
table-map (BGP)	1333
tacacs-server	1335
tagged-ieee-bpdu-enabled	1337
tcp burstrate	1338
telnet	1339
telnet server shutdown	1340
terminal	1341
threshold-monitor cpu	1342
threshold-monitor interface	1343
threshold-monitor memory	1346
threshold-monitor security	1348
threshold-monitor sfp	1350
timeout fnm	1353
timers	1354
timers (BGP)	1355
traceroute	1356
track	1357
transmit-holdcount	1359
transport-service	1360
trunk-enable	1361
udld enable	1362
unhide fips	1363
unlock username	1364
update-time (BGP)	1365
usb	1366
usb dir	1367
usb remove	1368
user (alias configuration)	1369
username	1370
username admin enable false	1372
username user enable false	1373
vc-link-init	1374
vcenter	1375
vcenter discovery (ignore delete responses)	1376
vcs (logical chassis cluster mode)	1377
vcs (standalone mode)	1379
vcs config snapshot (logical chassis cluster mode)	1381

vcs logical-chassis enable (fabric cluster mode)	1382
vcs rbridge-id (fabric cluster mode)	1383
vcs vcsid (fabric cluster mode)	1384
vcs virtual-fabric enable	1385
vcs replace rbridge-id	1386
vcs virtual ip	1387
virtual-fabric	1388
virtual-ip	1389
virtual-mac	1390
vlag ignore-split	1391
vlan classifier activate group	1392
vlan classifier group	1393
vlan classifier rule	1394
vlan dot1q tag native	1395
vlan-profile (AMPP)	1396
vnetwork vcenter discover	1397
vrf	1398
vrf-lite-capability (OSPF)	1399
vrrp-extended-group	1400
vrrp-group	1401
zoning defined-configuration alias	1402
zoning defined-configuration cfg	1404
zoning defined-configuration zone	1406
zoning enabled-configuration cfg-action cfg-clear	1408
zoning enabled-configuration cfg-action cfg-save	1409
zoning enabled-configuration cfg-action cfg-transaction-abort	1410
zoning enabled-configuration cfg-name	1411
zoning enabled-configuration default-zone-access	1412

About This Document

In this chapter

- How this document is organized xxxiii
- Supported hardware and software. xxxiii
- What's new in this document xxxiv
- Document conventions xxxiv
- Notice to the reader xxxvii
- Additional information. xxxvii
- Getting technical help xxxviii
- Document feedback xxxviii

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, 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 6740
 - Brocade VDX 6740-48
 - Brocade VDX 6740-64
- Brocade VDX 6740-T
 - Brocade VDX 6740T-48
 - Brocade VDX 6740T-64
 - Brocade VDX 6740T-1G
- Brocade VDX 8770
 - Brocade VDX 8770-4
 - Brocade VDX 8770-8

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

What's new in this document

This document supports the following new feature:

- VXLAN

NOTE

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
<i>italic text</i>	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. For example: command [active standby disabled] = One (and only one) of this set of keywords may be used. command [active] [standby] [disabled] = Three independent options, and one or more may be used on the same command line.
{ x y z }	A choice of required keywords appears in braces separated by vertical bars. You must select one. For example: command {active standby disabled} = One (and only one) of this set of keywords/operands must be used.
screen font	Examples of information displayed on the screen.
< >	Nonprinting characters, for example, passwords, appear in angle brackets.
[]	Default responses to system prompts appear in square brackets.
<i>italic text</i>	Identifies variables.
bold text	Identifies literal command options and keywords.

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.

Nesting square brackets and curly brackets

When reading a command entry, optional keywords are surrounded by square brackets and mandatory keywords are surrounded by curly brackets. See “Command syntax conventions” on page xxxv for complete details.

In some cases, these brackets can be nested. In this example, rbridge-id is optional as denoted by the square brackets, but if you use it, then you must follow it with either a specific rbridge-id or the word “all.”

Example

```
command [rbridge-id {rbridge-id | all}]
```

However, square brackets can appear within curly brackets, showing that while a keyword is mandatory, supporting operands may be optional, as shown below:

Example

```
command {security [active] [standby] [disabled]}
```

```
command {security [active | standby | disabled]}
```

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 xxxvii 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.

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.

Using the Network OS CLI

In this chapter

• DCB command line interface	1
• Saving your configuration changes	1
• Network OS CLI RBAC permissions	2
• Default roles	2
• Accessing the Network OS CLI through Telnet	2
• Network OS CLI command modes	3
• Network OS CLI keyboard shortcuts	8
• Using the do command as a shortcut	8
• Displaying Network OS CLI commands and command syntax	9
• Network OS CLI command completion	10
• Network OS CLI command output modifiers	10
• Show command output information	11

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 3.

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.

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 open Telnet sessions and issue commands using the privileged EXEC mode. Network OS supports up to 32 Telnet sessions with the admin login.

Network OS CLI command modes

The following lists the major 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.

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 privileged EXEC mode, enter the configure terminal command.	Configure features that affect the entire switch.
line vty	switch(config)# line vty exec-timeout 60 switch(config-line-vty)#	From global configuration mode, enter the line vty command.	Specify the amount of time a CLI session can be idle before it logs you out.
RBridge ID configuration mode	RBridge ID: switch (config)# rbridge-id 1 switch (config-rbridge-id-1)#	From global configuration mode, specify a node by entering the rbridge-id rbridge_id command, where <i>rbridge-id</i> is the RBridge ID of the selected node.	Configure features and issue show commands specific to an individual node in a Virtual Cluster Switching (VCS) environment. This includes both fabric cluster and management cluster scenarios.
Interface subtype	Port-channel: switch(config-Port-channel-63)# 10-Gigabit Ethernet (DCB port): switch(config-if-te-0/1)# VLAN:switch(config-Vlan-1)# VE: switch(config)# rbridge-id 11 switch(config-rbridge-id-11)# int ve 56 switch(config-Ve-56)#	From global configuration mode, specify an interface by entering one of the following commands: interface fcoe interface fortygigabitethernet interface gigabitethernet interface hundredgigabitethernet interface loopback interface port-channel interface tengigabitethernet interface ve interface vlan A virtual Ethernet (VE) interface can be configured in standalone or VCS mode (the latter is shown at left).	Access and configure individual interface subtypes. Enter ? at a command prompt to see what interface subtypes are available for that command.

1 Network OS CLI command modes

Network OS CLI command modes (Continued)

Command mode	Prompt	How to access the command mode	Description
Protocol configuration	LLDP: <code>switch(config-lldp) #</code> Spanning-tree: <code>switch(config-mstp) #</code> <code>switch(config-rstp) #</code> <code>switch(config-stp) #</code> <code>switch(config-pvst) #</code> <code>switch(config-rpvst) #</code> <code>switch(config-udld) #</code>	From 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 • protocol udld	Access and configure protocols.
FCoE configuration	FCoE: <code>switch(config-fcoe)#</code> FCoE fabric-map sub-mode: <code>switch(config-fcoe-fabric-map) #</code> FCoE map sub-mode: <code>switch(config-fcoe-map) #</code>	From global configuration mode, use the fcoe command to enter FCoE configuration mode. From 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.
Access Gateway (AG) configuration	AG configuration mode: <code>switch(config-rbridge-12-ag) #</code> N_Port configuration mode: <code>switch(config-rbridge-12-ag-nport-if-fi-port) #</code> Port Grouping configuration mode: <code>switch(config-rbridge-12-ag-pg-pgid) #</code>	From RBridge-ID configuration mode, enter the ag command. From AG configuration mode, enter the nport port command where <i>port</i> is an N_Port number supported by the hardware platform. From AG configuration mode, enter pg pgid where <i>pgid</i> is the port group identification number.	Access and configure Access Gateway features.
AMPP port-profile mode	AMPP port-profile: <code>switch(config-port-profile-name) #</code> VLAN-profile sub-mode: <code>switch(config-vlan-profile) #</code> QoS-profile sub-mode: <code>switch(config-qos-profile) #</code> FCoE-profile sub-mode: <code>switch(config-fcoe-profile) #</code> Security-profile sub-mode: <code>switch(config-security-profile) #</code>	From the global configuration mode, enter the port-profile command to enter port-profile configuration mode. From 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.

Network OS CLI command modes (Continued)

Command mode	Prompt	How to access the command mode	Description
Routing protocol configuration	BGP: switch(config)# switch(config-rbridge-id-1)# switch(config-bgp-router)#	From global configuration mode, specify an RBridge ID to enter RBridge ID configuration mode.	Configure Border Gateway Protocol routing protocol
	BGP route-map configuration mode: switch(config-rbridge-id-1)# switch(config-route-map-myroutemap/permit/1)#	From RBridge ID configuration mode, use the router bgp command to enter BGP configuration mode.	
	BGP address-family IPv4-unicast mode: switch(config-bgp-router)# switch(config-bgp-ipv4u)#	From RBridge ID configuration mode, use the route-map command with a permit or deny statement and an <i>instance number</i> to enter BGP route-map configuration mode., From BGP configuration mode, use the address-family ipv4 unicast command to enter BGP address-family IPv4 unicast configuration mode.	
	OSPF VRF: switch(config)# rbridge-id 5 switch(config-rbridge-id-5)# router ospf switch(config-router-ospf-vrf-default-vrf)#	From RBridge ID configuration mode, use the router ospf command to enter OSPF VRF configuration mode.	Configure Open Short Path First routing protocol
	PIM: switch(config)# rbridge-id 5 switch(config-rbridge-id-5)# router pim switch(conf-pim-router)#	From Bridge ID configuration mode, use the router pim command to enter PIM configuration mode.	Configure Protocol Independent Multicast routing protocol
Virtual-router-group configuration mode	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)#	From RBridge ID configuration mode, use the int ve command to enter VE configuration mode. Then use the vrrp-extended-group command to enter virtual-router-group configuration mode.	
DCB feature configuration	CEE map: switch(config-cee-map-default)# Standard ACL: switch(config-macl-std)# switch(config-ip-std)# Extended ACL: switch(config-macl-ext)# switch(config-ip-ext)#	From 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 • ip access-list standard • ip access-list extended	Access and configure CEE map features.
ELD configuration mode	switch(config)# protocol edge-loop-detection switch(config-eld)#	From global configuration mode, enter the protocol edge-loop-detection command.	Configure edge loop detection.

1 Network OS CLI command modes

Network OS CLI command modes (Continued)

Command mode	Prompt	How to access the command mode	Description
Hardware configuration	switch(config) # hardware	From global configuration mode, specify the hardware mode by entering the hardware command.	This mode is a prerequisite for entering connector and port-group mode.
Connector mode	switch# hardware connector switch(config-connector [n] /n/n) #	From hardware mode, specify the connector node and [rbridge-id]/slot/port information.	Connector mode is used to enable breakout on ports. When breakout is enabled, ports are appended in the output with a colon(:) followed by values 1-4. RBridge ID is not used in standalone mode.
DSCP mutation mapping	DSCP Mutation Map: switch(dscp-mutation-mapname) #	From global configuration mode, remap incoming DSCP values by entering the following command: qos map dscp-mutation mapname	
DSCP to CoS priority mapping	DSCP to CoS Map: switch(dscp-cos-mapname) #	From global configuration mode, create a DSCP to CoS priority map by entering the following command: qos map dscp-cos mapname	
DSCP to traffic class mapping	DSCP to Traffic Class Map: switch(dscp-traffic-class-mapname) #	From global configuration mode, create a DSCP to traffic class map by entering the following command: qos map dscp-traffic-class mapname	
Port-group configuration	switch(config-port-group-1/3/9) #	From hardware configuration mode, enter the port-group command followed by a port group identification: port-group rbridge-id/slot/port-group-id The port-group-id is specific to the Brocade VDX 8770 switch 27x40 GbE line card.	This mode allows you to enable Performance or Density operating modes on a specific port group on the 27x40 GbE line card only.
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 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 policy-class-map sub-mode from policy-map mode, enter class classmapname To enter the policy-class-map-policer attributes sub-mode from policy-map-class mode, enter police followed by the policing attributes.	

Network OS CLI command modes (Continued)

Command mode	Prompt	How to access the command mode	Description
Alias configuration	switch(config-alias-config) #	From global configuration mode, enter the alias-config command. Use the alias string expansion command to create aliases.	Access configure alias features.
User alias configuration	switch(config-alias-config-user) #	From alias configuration mode, enter the user name command.	Access configure user alias features.
Polycymap configuration	switch(config-polycymap) #	From global configuration mode, enter the policy-map name command.	
Polycymap class map configuration	switch(config-polycymap-class) #	From polycymap configuration mode, enter the class name command.	
Polycymap class police configuration	switch(config-polycymap-class-police) #	From polycymap class configuration mode, enter the police cir value command.	
VCS configuration mode	switch(config-vcs) #	From privileged EXEC mode, enter the vcs vcsid id-number logical-chassis enable command	
VRF configuration mode	(config-rbridge-12-vrf-vrf_name) #	From RBridge ID configuration mode, enter the vrf name command.	

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 1 lists Network OS CLI keyboard shortcuts. Keystroke keys are not case-sensitive.

TABLE 1 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.
Ctrl+C	Returns to privileged EXEC mode.
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 for the current session.

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-lddp)# 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  802.1x configuration
dpod   Provides DPOD license information.
```

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)
```

1 Network OS CLI command completion

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.

```
Possible completions:
lacp      LACP commands
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 2](#).

TABLE 2 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.

TABLE 2 CEE CLI command output modifiers (Continued)

Output modifier	Description
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 <i>string</i>	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.
more	Paginates the output.
nomore	Suppresses the pagination of the output.
FLASH	Redirects the output to flash memory.

Show command output information

Network OS contains many versions of the **show** command. The output of the **show** command changes depending on your configuration and situation. However, in general terms the **show** command falls into one of two categories.

Any **show** commands that are fabric (global configuration) in nature like VLAN, MAC Address table, AMPP, Zoning, and so on should display or clear the information for all nodes in a logical chassis.

Any **show** commands that are local to a switch (such as Layer 3 or Layer 2 functionality like sFlow, SPAN, and so on,) should display the local information by default, and display different switch information based on the **rbridge-id** option.

1 Show command output information

Network OS Commands

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 a start-stop packet upon completion of a command or login.
	none	Disables accounting. This is functionally equivalent to the no form of the commands.
	tacacs+	Uses the TACACS+ server for accounting.

Defaults AAA accounting is disabled.

Command Modes Global configuration mode

Description Use this command to enable or disable 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.

Enter **no aaa accounting exec default start-stop tacacs+** to disable login accounting.

Enter **no aaa accounting commands default start-stop tacacs+** to disable command accounting.

You can also use the optional "none" parameter for either command (instead of the **no** parameter) to disable that accounting.

2 aaa 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** form of the command:

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

To disable command accounting using the **none** parameter:

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

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

aaa authentication

Configures the AAA login sequence.

Synopsis **aaa authentication login** {default | ldap | local | radius {local | local-auth-fallback} | tacacs+ {local | local-auth-fallback}}

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 to use the local switch database if prior authentication methods are inactive.

local-auth-fallback Specifies to use the local switch database if prior authentication methods are not active or if authentication fails.

local Specifies the local switch database.

radius Specifies the RADIUS servers.

local Specifies to use the local switch database if prior authentication methods are inactive.

local-auth-fallback Specifies to use the local switch database if prior authentication methods are not active or if authentication fails.

tacacs+ Specifies the TACACS+ servers.

local Specifies to use the local switch database if prior authentication methods are inactive.

local-auth-fallback Specifies to use the local switch database if prior authentication methods are not active or if authentication fails.

Defaults 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.

2 aaa authentication

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.

Beginning with Network OS v4.0.0, when the local option is specified as a secondary authentication service, local authentication is tried only when the primary AAA authentication service (TACACS+/Radius/LDAP) is either unreachable or not available. Local authentication will not be attempted if the authentication with the primary service fails.

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...
```

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**

access-group

Applies or removes an ACL from an interface.

Synopsis {ip | ipv6 | mac} **access-group** NAME {in | out}
 no {ip | ipv6 | mac} **access-group** NAME {in | out}

Operands ip | ipv6 | mac Specifies the Layer 2 or Layer 3 ACL to bind to an interface.
 in | out Specifies the ACL binding direction (ingress or egress).
 access group NAME Specifies the name assigned to the access group.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to apply an ACL to an interface.

Usage Guidelines Use the **no** form of this command to remove an ACL from an interface.

Examples None

See Also None

access-list

Creates an ACL.

Synopsis `{ip | ipv6 | mac} access-list {standard | extended} NAME`
`no {ip | mac} access-list {standard | extended} NAME`

Operands `ip | ipv6 | mac` Displays the configured rules of either a Layer 2 or Layer 3 ACL.
`standard | extended` Specifies the ACL type.
`access-list NAME` Specifies the name assigned to the access list.

Defaults None

Command Modes Global configuration mode

Description Use this command to create an ACL on an interface.

Usage Guidelines Use the **no** form of this command to remove an ACL from an interface.

Examples None

See Also None

activate (NSX Controller connection profile)

Activates an NSX controller connection profile.

Synopsis **activate**
 no activate

Operands None

Defaults Profile is inactive.

Command Modes NSX Controller configuration mode

Description Use this command to activate the profile, thereby initiating the connection between the NSX controller and the VCS fabric.

Usage Guidelines This command is allowed for a switch that is in logical chassis cluster mode only.
You must configure the NSX Controller IP address before executing this command.
You must configure the VCS virtual IP address of the cluster before executing this command.
Use the **no** form of the command to mark the connection profile inactive. Any existing connection is closed. However, all tunnels already created by the NSX controller remain open.

Examples To activate an NSX controller connection profile that you have created and named *profile1*:

```
switch# configuration  
switch(config)# nsx-controller profile1  
switch(config-nsx-controller-profile1)# activate
```

See Also

2 activate (VXLAN gateway)

activate (VXLAN gateway)

Activates a gateway instance.

Synopsis **activate**
 no activate

Operands None

Defaults None

Command Modes VXLAN gateway configuration mode

Description Use this command to activate this gateway instance. By default, a gateway is not activated during initial configuration. It is recommended to configure all gateway parameters before activating the gateway. This operation enables all tunnels that are associated with this gateway. VXLAN tunnels are not user configurable.

Usage Guidelines The IP address of the gateway must already be configured (with the **ip interface** command).

If Rbridge attachments are configured for this gateway, the VE, VRID and VRF configurations must match on all such Rbridges.

The **no** form of this command deactivates the gateway. All associated tunnels are also deactivated.

Examples To activate a gateway that you have configured with the name of *gateway1*:

```
switch# configure  
switch(config)# overlay-gateway gateway1  
switch(config-overlay-gw-gateway1)# activate
```

See Also

address-family ipv4 unicast (BGP)

Enables IPv4 address-family support for BGP4 routing.

Synopsis **address-family {ipv4} {unicast}**
no address-family {ipv4} {unicast}

Operands None

Defaults None

Command Modes BGP configuration mode

Description Use this command to enter IPv4 address-family configuration mode to configure a variety of BGP4 unicast routing options.

Usage Guidelines Use the **no** form of this command to remove IPv4 address-family configurations from the device.

Examples To enable BGP IPv4 address-family configuration mode:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# address-family ipv4 unicast  
switch(config-bgp-ipv4u)#
```

See Also None

address-family ipv4 unicast (VRF)

Enables IPv4 address-family support for VRF routing.

Synopsis **address-family {ipv4} {unicast}**
 no address-family {ipv4} {unicast}

Operands None

Defaults None

Command Modes VRF configuration mode

Description Use this command to enter IPv4 address-family configuration mode to configure a variety of VRF unicast routing options.

Usage Guidelines Use the **no** form of this command to remove IPv4 address-family configurations from the device.

Examples To enable BGP IPv4 address-family configuration mode:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# vrf orange
switch(config-vrf-orange)# address-family ipv4 unicast
switch(config-ipv4u)#
```

See Also None

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.

Usage Guidelines Enter **no advertise dcbx-fcoe-app-tlv** to return to the default setting.

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 Enter **no advertise dcbx-fcoe-logical-link-tlv** 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 Type, Length, Values (TLV) values.

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 Use this command to advertise 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 Enter **no advertise dcbx-iscsi-app-tlv** 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 (TLV) values.

Synopsis	advertise dcbx-tlv
	no advertise dcbx-tlv
Operands	None
Defaults	Advertise is enabled.
Command Modes	Protocol LLDP configuration mode
Description	Use this command to advertise to any attached device the mandatory Data Center Bridging eXchange protocol (DCBX) Type, Length, Values (TLV) values.
Usage Guidelines	Enter no advertise dcbx-tlv to return to the default setting.
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, Values (TLV) values.

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, Values (TLV) values.

Usage Guidelines Enter **no advertise dot1-tlv** to return to the default setting.

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, Values (TLV) values.

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, Values (TLV) values.

Usage Guidelines Enter **no advertise dot3-tlv** to return to the default setting.

Examples None

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

advertise optional-tlv

Advertises the optional Type, Length, and Values (TLV) values.

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 described optional TLVs.

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

Examples None

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

advertise-backup

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

Synopsis **advertise-backup**
 no advertise backup

Operands There are no operands for this command.

Defaults Advertisement is disabled.

Command Modes Virtual-router-group configuration mode

Description Use this command to enable a backup VRRP 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.

Usage Guidelines This command can be used for VRRP-E, but not for VRRP.
Enter **no advertise backup** to return to the default setting (no periodic transmission).

Examples To enable the backup VRRP routers to send advertisement frames to the master VRRP 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 **advertisement-interval (VRRP), backup-advertisement-interval, vrrp-extended-group**

advertisement interval (fabric-map)

Configures the FIP advertisement interval.

Synopsis **advertisement interval** *milliseconds*
no advertisement interval

Operands *milliseconds* The interval value in milliseconds. Valid values range from 250 through 90000 milliseconds.

Defaults 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 You must be in the feature configuration mode for FCoE fabric-map for this command to function.
Enter **no advertisement interval** return to the default setting.

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 VRRP router advertises its existence to the backup routers.

Synopsis **advertisement-interval** *range*

Operands *range* Interval at which the master VRRP router advertises its existence to the backup routers. Valid values range from 1 through 255 seconds.

Defaults 1 second

Command Modes Virtual-router-group configuration mode

Description Use this command to configure the advertisement interval of the master VRRP router. This interval is the length of time, in seconds, between each advertisement sent from the master to its backup VRRP 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 **backup-advertisement-interval**, **vrrp-extended-group**, **vrrp-group**

ag

Enables Access Gateway (AG) configuration mode.

Synopsis ag

Operands None

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command while in RBridge ID configuration mode for a specific RBridge ID. This command enables Access Gateway (AG) configuration mode on a specific switch. In this mode, you can configure Access Gateway features such as Access Gateway policies, VF_Port to N_Port mapping, Port Grouping, N_Port Monitoring reliability counters, and Modified Managed Fabric Name Monitoring (N-MFNM) mode timeout values.

Usage Guidelines None

Examples Enabling AG configuration mode while in RBridge ID configuration mode.

```
sw0(config-rbridge-id-2)# ag
sw0(config-rbridge-id-2-ag)#
```

See Also **show ag**

ag enable

Enables Access Gateway mode on a switch.

Synopsis **ag** [**rbridge-id** *rbridge id* **vcs-id** *vcs-id*] **enable**
no ag enable

Operands **rbridge-id** *rbridge-id* Specifies the RBridge identifier for the switch.
vcs-id *vcs-id* Specifies the VCS identifier for the switch.

Defaults AG mode is disabled.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable Access Gateway mode on the switch. Enabling AG mode enables VDX 6730 switch FC ports, configures them as N_Ports, and then maps these N_Ports to VF_Ports using a default mapping configuration based on the switch platform. Enabling Access Gateway mode reboots the switch.

Usage Guidelines Enter the **ag enable** command to enable Access Gateway mode on a switch that is in VCS mode.
 Enter the **ag rbridge-id rbridge id vcs-id vcs-id enable** command to enable VCS mode and Access Gateway mode on a standalone switch.
 Enter the **no ag enable** command to disable Access Gateway mode.
 The switch must be in VCS mode to enable Access Gateway.

Examples The following example enables AG mode on a local switch:

```
switch# ag enable
```

 The following example enables AG mode on a specific switch using the Rbridge ID and VCS ID:

```
switch# ag rbridge-id 1 vcs-id 2000 enable
```

 The following example disables AG mode on a local switch:

```
switch# no ag enable
```

See Also **show ag**

aggregate-address (BGP)

Configures the device to aggregate routes from a range of networks into a single network prefix.

Synopsis **aggregate-address** *ip-addr ip-mask* [**as-set**] [**summary-only**] [**suppress-map** *map-name*]
 [**advertise-map** *map-name* [**attribute-map** *map-name*]]

no aggregate-address

Operands	<i>ip-addr</i>	IPv4 address.
	as-set	Causes the device to aggregate AS-path information for all routes in the aggregate routes from a range of networks into a single network prefix.
	summary-only	Prevents the device from advertising more-specific routes contained within the aggregate route.
	suppress-map	Prevents the more-specific routes contained in the specified route map from being advertised.
	advertise-map	Causes the device to advertise the more-specific routes in the specified route map.
	attribute-map	Causes the device to set attributes for the aggregate routes according to the specified route map.
	<i>map-name</i>	Specifies a route map to be consulted.

Defaults This feature is disabled.

Command Modes BGP address-family IPv4 unicast configuration mode

Description By default, the device advertises individual routes for all networks. Use this command to configure the device to aggregate routes from a range of networks into a single network prefix.

Usage Guidelines Use the **no** form of this command to restore the defaults.

Examples To aggregate routes from a range of networks into a single network prefix and prevent the device from advertising more-specific routes:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# aggregate-address 10.11.12.0 summary-only
```

See Also **route-map**

alias

Configures the global or user switch alias.

Synopsis **alias** *string expansion*

no alias *string expansion*

Operands *string* Alias name string. The number of characters can be from 1 through 64.
 expansion Commands for the alias name. Multiple commands can be separated with a semicolon (;).

Defaults None

Command Modes Alias configuration mode
 User-alias configuration mode

Description Use this command to configure global or user-level alias for switch commands. The global name is visible to all users. When the global alias name is called, the configured alias expansion commands are executed on the prompt.

Usage Guidelines The global alias is accessible across all users.
 The user-level alias is accessible only when the respective user logs in.
 Use the **no** form of this command to remove the alias. You must be in the correct configuration mode in order to remove the global or user alias.

Examples The following example sets both a switch alias and a user alias.
 switch(config)# **alias-config**
 switch(config-alias-config)# **alias user-alias "show clock"**
 switch(config-alias-config)# **alias company Brocade**
 switch(config-alias-config)# **alias redwood engineering**
 switch(config-alias-config)# **user john smith**
 switch(config-alias-config-user)# **alias manager engineering**

See Also **alias-config**, **user** (alias configuration)

alias-config

Launches the alias configuration mode.

Synopsis **alias-config**

Operands None

Defaults None

Command Modes Global configuration mode

Description Use this command to launch alias configuration mode. This mode allows you to configure the alias for the switch.

Usage Guidelines None

Examples Example of setting a switch alias and a user alias.

```
switch(config)# alias-config
switch(config-alias-config)# alias user-alias "show clock"
switch(config-alias-config)# alias company Brocade
switch(config-alias-config)# alias redwood engineering
switch(config-alias-config)# user john smith
switch(config-alias-config-user)# alias manager engineering
```

See Also **alias, user (alias configuration)**

allow non-profiled-macs

Specifies whether non-profiled MAC addresses on the profiled port are dropped.

Synopsis **allow non-profiled-macs**
 no allow non-profiled-macs

Operands None

Defaults Non-profiled MAC addresses are not dropped.

Command Modes Port-profile mode

Description Use this command to decide whether non-profiled MAC addresses on profiled port should be dropped or not. This configuration is allowed on the default profile only.

Usage Guidelines Enter **no allow non-profiled-macs** to return to the default setting.

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

See Also None

always-compare-med (BGP)

Configures the device always to compare the Multi-Exit Discriminators (MEDs), regardless of the autonomous system (AS) information in the paths.

Synopsis **always-compare-med**
 no always-compare-med

Operands None

Defaults This feature is disabled.

Command Modes BGP configuration mode

Description Use this command to configure the device to compare the Multi-Exit Discriminators (MEDs), regardless of the AS information in the paths.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To configure the device always to compare the MEDs:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# always-compare-med
```

See Also None

always-propagate (BGP)

Enables the device to reflect routes even though they are not installed in the Routing Table Manager (RTM).

Synopsis **always-propagate**
 no always-propagate

Operands None

Defaults This feature is disabled.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to enable the device to reflect routes even though they are not installed in the RTM.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To configure the device to reflect routes that are not installed in the RTM:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# address-family ipv4 unicast  
switch(config-bgp-ipv4u)# always-propagate
```

See Also None

area nssa (OSPF)

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**}
no area nssa

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 parameter 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.
Note: This parameter is disabled by default, which means the default route must use a Type 7 LSA.

default-information-originate

When configured on the ABR, this parameter 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. By default the NSSA ABR does not originate a default route to the NSSA.

Defaults No areas are created.

Command Modes OSPF VRF router configuration mode

Description Use this command to create an NSSA area or modify 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 Enter **no area nssa** to delete an NSSA.

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

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# area 2 nssa 5 no-summary
```

See Also None

area range (OSPF)

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** | **cost** *cost_value* | **not-advertise**}
no area range

Operands	<i>A.B.C.D</i>	Area address in dotted decimal format.
	<i>decimal</i>	Area address in decimal format.
	<i>E.F.G.H I.J.K.L</i>	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 <i>advertise</i> and generates a Type 3 summary LSA.
	cost <i>cost_value</i>	Sets the cost value for the area range. This value is used as the generated summary LSA cost. The range for <i>cost_value</i> is 1 to 6777214.
		If this value is not specified, the cost value is the default range metric calculation for the generated summary LSA cost.
	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.

Defaults None

Command Modes OSPF VRF router configuration mode

Description Use this command 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 Enter **no area range** 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# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# area 3 range 1.1.1.0 255.255.255.0 advertise
```

See Also None

area stub (OSPF)

Creates a stub area or modifies its parameters.

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

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 parameter makes the area a so-called totally stubby area, which can only have Types 1 and 2. This parameter is disabled by default.

Defaults No areas are created.

Command Modes OSPF VRF router configuration mode

Description Use this command to create or delete a stub area or modify 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 Enter **no area stub** to delete a stub area.

Examples To set an additional cost of 5 on a stub area called 2 (in decimal format):

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# area 2 stub 5
```

See Also None

area virtual-link (OSPF)

Creates or modifies virtual links for an area.

Synopsis	area { <i>A.B.C.D</i> <i>decimal</i> } virtual-link <i>E.F.G.H</i> [authentication-key { 0 2 255 } <i>password</i>] [dead-interval <i>time</i>] [hello-interval <i>time</i>] [md5-authentication { key-activation-wait-time <i>time</i> key-id <i>num key</i> }] [retransmit-interval <i>time</i>] [transmit-delay <i>time</i>] no area virtual-link	
Operands	<i>A.B.C.D</i>	Area address in dotted decimal format.
	<i>decimal</i>	Area address in decimal format.
	<i>E.F.G.H</i>	ID of the OSPF router at the remote end of the virtual link.
	authentication-key	Sets the 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.
	<i>password</i>	OSPF password. The password can be up to eight alphanumeric characters.
	dead-interval <i>time</i>	How long 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. Valid values range from 3 through 65535 seconds. The default is 40 seconds.
	hello-interval	Time 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. Valid values range from 1 through 65535 seconds. The default is 10 seconds.
	md5-authentication	Sets either MD5 key-activation wait time or key identifier.
	key-activation-wait-time <i>time</i>	Time 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 (300 seconds) after the new MD5 key is in operation. Valid values range from 0 through 14400 seconds. The default is 300 seconds.
	key-id <i>num key</i>	The <i>num</i> is a number between 1 and 255 which identifies the MD5 key being used. This parameter is required to differentiate among multiple keys defined on a router. When MD5 is enabled, the <i>key</i> 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 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. Valid values range from 0 through 3600 seconds. The default is 5 seconds.

transmit-delay *time*

Estimated time 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 is incremented by the value of this parameter before transmission occurs. Valid values range from 0 through 3600 seconds. The default is 1 second.

Defaults No virtual links are created.

Refer to the Operands for specific defaults.

Command Modes OSPF VRF router configuration mode

Description Use this command to create or modify virtual links for an area.

Usage Guidelines Enter **no area virtual-link** 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# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# area 1 virtual-link 10.1.2.3
```

See Also None

2 arp

arp

Enables specification of an IPv4 address for an Address Resolution Protocol (ARP) entry.

Synopsis **arp** *A.B.C.D mac_address*

Operands *A.B.C.D* A valid IP address.
 mac_address A valid MAC address.

Defaults None

Command Modes RBridge configuration mode

Description Use this command to specify an IPv4 address for an ARP entry.

Usage Guidelines None

Examples None

See Also None

as-path-ignore (BGP)

Disables the comparison of the autonomous system (AS) path lengths of otherwise equal paths.

Synopsis **as-path-ignore**
 no as-path-ignore

Operands None

Defaults This feature is disabled.

Command Modes BGP configuration mode

Description Use this command to disable the comparison of the AS path lengths of otherwise equal paths.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To configure the device always to disable the comparison of AS path lengths:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# as-path-ignore
```

See Also None

attach rbridge-id

Assigns a range of Rbridge IDs to the VXLAN gateway instance.

Synopsis **attach rbridge-id {add | remove} *rb-range***

Operands

add	Attaches a specified range of Rbridge IDs to the VXLAN gateway.
remove	Un-attaches a specified range of Rbridge IDs from the VXLAN gateway.
<i>rb-range</i>	Specifies a range of RBridge IDs to attach to the VXLAN gateway. (You can also specify just one RBridge ID.) Ranges can be specified with hyphens, separated by commas, or contain a mixture of both. Do not use a space after a comma when specifying a range of IDs. For example, to specify RBridges 5 through 10 and RBridge 15, enter: 5-10,15.

Defaults None

Command Modes VXLAN Gateway Configuration mode

Description

Use this command to create a VXLAN overlay gateway instance for the Rbridges that you specify. You can configure other properties for the gateway instance while in VXLAN Gateway Configuration mode, but the gateway instance is not created until you run the **attach rbridge-id** command.

Use the **add** form of the command to attach Rbridge IDs to the VXLAN gateway, and use the **remove** form of the command to un-attach RBridge IDs from the VXLAN gateway.

When un-attaching Rbridge IDs, gateway and tunnel configurations on the specified Rbridge IDs are deleted.

Usage Guidelines

The Rbridge IDs that you specify must already be known to the cluster. (Rbridge IDs that have been removed from the cluster with the **no vcs enable rbridge-id** command cannot be used to attach to the VXLAN gateway.)

This command is allowed for a switch that is in logical chassis cluster mode only.

The Rbridge IDs that you specify must be on a VXLAN-capable gateway (either the Brocade VDX 6740 or VDX 6740-T), and the gateway must have a VCS license.

Examples

To add an Rbridge ID range of 10 through 30 on a VXLAN overlay gateway instance named *gateway1*:

```
switch# configure
switch(config)# overlay-gateway gateway1
switch(config-overlay-gateway1)# attach rbridge-id add 2-3
```

See Also

attach vlan

Identifies exported VLANs.

Synopsis **attach vlan** *vlan_ID* [**mac** *mac_ID*]
 no attach vlan *vlan_ID*

Operands **vlan** *vlan_ID* Specifies the VLAN ID of the VXLAN gateway. This can be a range, such as 5, 10, 20-25.
 mac *mac_ID* Specifies specific MAC address(es) of the VXLAN gateway.

Defaults None

Command Modes VXLAN Gateway Configuration mode

Description Use this command to identify the exported VLANs (these are VLANs than can be mapped to VXLAN domains). All the MAC addresses that the VXLAN gateway learns on these VLANs are shared with NSX. The command can optionally accept specific MACs, which can be shared with NSX. If the user specifies MAC addresses, only these specified MACs are shared with NSX for this VLAN.

Usage Guidelines The specified VLAN must already be configured.

You cannot run two forms of this command using the same VLAN IDs. For example, the commands **attach vlan x** and **attach vlan x mac y** cannot co-exist. If one form of the configuration exists, the other form of the configuration for the same VLAN ID is rejected.

Also, you cannot specify a VLAN range and a MAC address on the same command line. You can, however, specify a single VLAN ID and a MAC address on the same command line.

The **no** form of this command stops the MACs behind the specified VLANs from being shared with the NSX controller.

The deletion of a VLAN specified with this command is not allowed. For example, if you run the command **attach vlan x**, you cannot delete the exported VLAN called x by running the **no interface vlan x** command.

Examples To identify exported VLAN IDs and to specify a MAC address for the VXLAN gateway already configured and named *gateway1*:

```
switch# configure
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# attach vlan 5 mac 00:05:1e:c5:96:a4
```

See Also

auto-cost reference-bandwidth (OSPF)

Configures reference bandwidth.

Synopsis	auto-cost reference-bandwidth {ref-bw use-active-ports}	
	no auto-cost reference-bandwidth	
Operands	ref-bw	Reference bandwidth in Mbps. Valid values range from 1 through 4294967.
	use-active-ports	When set, any dynamic change in bandwidth immediately affects the cost of OSPF routes. This parameter enables cost calculation for currently active ports only.
Defaults	Reference bandwidth is 100 Mbps.	
Command Modes	OSPF VRF router configuration mode	
Description	Use this command to configure 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.	
	Enter no auto-cost reference-bandwidth to disable bandwidth configuration.	
Examples	To change a reference bandwidth of 500:	
	<pre>switch# configure switch(config)# rbridge-id 5 switch(config-rbridge-id-5)#router ospf switch(config-router-ospf-vrf-default-vrf)# auto-cost reference-bandwidth 500</pre>	
	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	

backup-advertisement-interval

Configures the interval at which backup VRRP routers advertise their existence to the master router.

Synopsis **backup-advertisement-interval** *interval*

Operands *interval* Interval at which a backup VRRP router advertises its existence to the master router. Valid values range from 60 through 3600 seconds.

Defaults 60 seconds

Command Modes Virtual-router-group configuration mode

Description Use this command to configure the advertisement interval of the backup VRRP routers. This interval is the length of time, in seconds, between each advertisement sent from the backup routers to the master router. The advertisement notifies the master router that the backup is still active. If the master router does not receive an advertisement from the backup 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 backup advertisement interval to 120 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)# backup-advertisement-interval 120
```

See Also **vrrp-group**, **vrrp-extended-group**

banner incoming

Sets the incoming banner message.

Synopsis **banner incoming** *message*
no banner incoming

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 the incoming banner. A banner is a text message that displays on the console. The banner can include information about the switch for a user to know when accessing the switch.

Usage Guidelines The banner must be from 1 through 2048 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 None

See Also None

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 2048 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
-----
```

2 banner login

```
Welcome to NOS CLI
user connected from ::FFFF:10.103.8.61 using ssh on abc.com
switch#
```

See Also **show running-config banner**

banner motd

Sets the message of the day (MOTD) banner.

Synopsis **banner motd** *message*
 no banner motd

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 the MOTD banner. A banner is a text message that displays on the console. The banner can include information about the switch for a user to know when accessing the switch.

Usage Guidelines The banner must be from 1 through 2048 characters in length. The banner can appear on multiple lines if you enter multiline mode by using **ESC+M** and exit by using **CTRL+D**.

Examples None

See Also None

bgp-redistribute-internal (BGP)

Causes the device to allow the redistribution of IBGP routes from BGP4 into RIP, OSPF, or ISIS.

Synopsis **bgp-redistribute-internal**
 no bgp-redistribute-internal

Operands None

Defaults This feature is disabled.

Command Modes BGP address-family IPv4 unicast configuration mode

Description By default, with default VRF instances, the device does not allow the redistribution of IBGP routes from BGP4 into RIP, OSPF, or ISIS. This helps to eliminate routing loops. In non-default VRF instances, the device does allow the redistribution of IBGP routes from BGP4 into RIP and OSPF. Use this command to redistribute BGP4 routes into OSPF, RIP, and ISIS.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples To configure a static network and change the administrative distance:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# bgp-redistribute-internal
```

See Also None

bind

Used to create a persistent binding between the logical FCoE port and the ten/forty gigabit or LAG port.

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

Operands **fortygigabitethernet** *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.

port-channel *number* Specifies a port-channel interface.

tengigabitethernet *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.*rbridge-id* Specifies the RBridge ID. 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 subtype configuration mode

Description Use this command to create a persistent binding between the logical FCoE port and the ten/forty gigabitethernet or LAG port. This will be stored in the configuration and retained across reboots.

Usage Guidelines When the FCoE logical port is automatically bound to a TE/FO 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.

ATTENTION

Only one type of binding can be used for each physical port, so the ten/forty gigabitethernet or LAG (MAC) binding configurations 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 None

bpdudrop enable

Drops STP, RSTP, MSTP, and PVST and RPVST bridge protocol data units (BPDUs), disabling the tunneling of those protocols on an interface.

Synopsis **bpdudrop enable** [rx | tx | all]
no bpdudrop enable [rx | tx | all]

Operands

tx	Disables tunneling in the transmit direction.
rx	Disables tunneling in the receive direction.
all	Disables tunneling in both the transmit and receive directions.

Defaults BPDUDROP is disabled.

Command Modes Interface subtype configuration mode

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 BPDUDROP enabled, the interface drops the BPDU frames, but does not shut down.

Usage Guidelines Enter **bpdudrop enable** with the **tx**, **rx**, or **all** options. Without an optional keyword, the action applies to the ingress direction only.

Enter **no bpdudrop enable** with the **tx**, **rx**, or **all** options to disable BPDU drop in one or more directions.

Enter **no bpdudrop enable** to disable BPDUDROP completely.

Examples To enable BPDUDROP on a specific 10-gigabit Ethernet interface:

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

To disable BPDUDROP on a specific port-channel interface:

```
switch(config)# interface port-channel 62
switch(conf-port-channel-62)# no bpdudrop enable
```

To disable BPDUDROP on a specific port-channel interface in the transmit direction:

```
switch(config)# interface port-channel 62
switch(conf-port-channel-62)# no bpdudrop enable tx
```

See Also interface

bridge-priority

Specifies the priority of the bridge.

Synopsis **bridge-priority** *priority*
 no bridge-priority

Operands *priority* Specifies the bridge priority. Valid values range from 0 through 61440 in increments of 4096.

Defaults 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.

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.

 If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

 Enter **no bridge-priority** to return to the default priority.

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**

capability as4 (BGP)

Enables 4-byte autonomous system number (ASN) capability at the BGP global level.

Synopsis **capability as4 {enable}**
 no capability as4

Operands **enable** Enables 4-byte ASN capability at the BGP global level.

Defaults This feature is disabled.

Command Modes BGP configuration mode

Description Use this command to enable 4-byte ASN capability at the BGP global level.

Usage Guidelines Use the **no** form of this command to disable this functionality.

Examples To enable 4-byte ASN capability:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# capability as4 enable
```

See Also None

capture packet interface

Enables the capture of packet information on an interface, for display on the switch itself or for storage in an automatically generated file.

Synopsis **capture packet** {**interface**} {**all** | **fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port*} {**direction** {**both** | **rx** | **tx**} {**filter** {**I2** | **I3** | **all**}}

Operands	interface	Selects an interface (required).
	all	Selects all interfaces.
	fortygigabitethernet	Selects a 40-GbE interface.
	gigabitethernet	Selects a 1-GbE interface.
	tengigabitethernet	Selects a 10-GbE interface.
	<i>rbridge-id/slot/port</i>	Selects the RBridge ID, slot, and port of the respective interface.
	direction	Selects a direction (required).
	both	Selects traffic in both transmit and receive directions.
	rx	Selects received traffic.
	tx	Selects transmitted traffic.
	filter	Selects the packet types to be filtered (required).
	I2	Filters only Layer 2 packets to the CPU.
	I3	Filters only Layer 3 packets to the CPU.
	all	Filters all packets to the CPU, including transit packets if an access control list (ACL) is enabled (Refer to the Usage Guidelines.)

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to capture packet information on an interface. This can provide significant help in debugging, especially for Layer 2 TRILL and Layer 3 packets. Captured packets are stored in a circular buffer, and they are also written to an automatically generated “pktcapture.pcap” file, which can store up to 1500 K of data in flash memory (the equivalent of approximately 10k packets, each having an average size of 100 bytes). Once this file is full, it is saved at *_old.pcap and data are written to a new pktcapture.pcap file. These files can be exported and viewed through a packet analyzer such as Wireshark.

NOTE

Up to 100 packets per interface can be captured. Once the buffer is filled, the oldest packets are replaced with the most recent.

Usage Guidelines This command is supported in VCS and standalone modes. This command can be entered on any RBridge in a Brocade VCS Fabric.

To disable packet capture globally, use the **no capture packet all** command.

NOTE

The **all** option is not supported for enabling packet capture.

To view the captured information on the switch, use the **show capture packet interface** command.

Note the following limitations:

- Support is provided only on physical interfaces (1-, 10-, and 40-gigabit Ethernet), not on logical interfaces. To see packets on logical interfaces, first enable the capture on the corresponding physical interfaces.
- In the initial release, support for capturing transit traffic requires ACL logging.
- Packets that are dropped in the ASIC cannot be captured.



CAUTION

Capturing packets over multiple sessions and over long durations can affect system performance.

Examples `switch# capture packet interface tengigabitethernet 166/0/1 direction both
filter all`

See Also `show capture packet`

cbs

Mandatory command for configuring the controlled burst size for a class-map.

Synopsis **cbs** *cbs-size*
 no cbs *cbs-size*

Operands *cbs-size* Controlled burst size. Valid values range from 1250 through 5000000000 bytes in increments of 1 byte. This is a mandatory parameter for configuring a class-map.

Defaults None

Command Modes Polycymap class police configuration mode

Description This command sets the controlled burst size for a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples This example configures a class-map called “default” within a policy-map.

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# cbs 50000
```

See Also **conform-set-dscp, conform-set-prec, conform-set-tc, ebs, eir, exceed-set-dscp, exceed-set-prec, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy, set-priority**

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 subtype configuration mode

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.
Enter **no cee** to remove the CEE Provisioning map.

Examples To apply a CEE map to a specific 10-gigabit Ethernet 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	Use this command to enter the CEE map configuration mode.																											
Usage Guidelines	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, BW% 40 2: Weight 60, PFC Disabled, 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 <table><tr><td>CoS:</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td></tr><tr><td colspan="9">-----</td></tr><tr><td>PGID:</td><td>2</td><td>2</td><td>2</td><td>1</td><td>2</td><td>2</td><td>2</td><td>2</td></tr></table> Enabled on the following interfaces	CoS:	0	1	2	3	4	5	6	7	-----									PGID:	2	2	2	1	2	2	2	2
CoS:	0	1	2	3	4	5	6	7																				

PGID:	2	2	2	1	2	2	2	2																				
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**
 no cee-map default

Operands None

Defaults The only map name allowed is “default.”

Command Modes FCoE map configuration mode

Description Use this command to assign a cee-map to the FCoE fabric-map.

Usage Guidelines You must be in the feature configuration mode for FCoE map for this command to function.
 Enter **no cee-map** to revert to the default values for the map.

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 ssh`

`certutil import ldapca | syslogca directory ca certificate path protocol {FTP | SCP} host remote_ip user user_acct password password [rbridge-id {rbridge_id | all}]`

`no certutil ldapca [rbridge-id {rbridge-id | all}]`

Operands

directory path	Specifies the path to the certificate.
file filename	Specifies the filename for the certificate.
host remote_ip	Specifies the IP address of the remote host.
password password	Specifies the password to access the remote host.
protocol FTP SCP	Specifies the protocol used to access the remote server.
rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
rbridge-id	Specifies a unique identifier for a node.
all	Specifies all identifiers for a node.
user user_acct	Specifies the user name 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 Enter `no certutil ldapca` to delete the LDAP CA certificates of all Active Directory (AD) servers. The `rbridge-id` operand is supported in VCS mode only.

Examples In Standalone mode

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 import the SSH public key for user "admin" from the remote host:

```
switch# certutil import sshkey user admin host 10.70.4.106 directory
/users/home40/bmeenaks/.ssh file id_rsa.pub login fvt
Password: *****
switch# 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX6720-60, Event: sshutil,
Status: success, Info: Imported SSH public key from 10.70.4.106 for user 'admin'.
switch#
```

To delete all LDAP CA certificates:

```
switch# no certutil ldapca
```

2 certutil import ldapca

In VCS mode

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 rbridge-id 3
password:
switch#
```

To delete LDAP certificates on rbridge-id 3:

```
switch# no certutil syslogca rbridge-id 3
Do you want to delete syslogca certificate? [y/n]:y
Warning: All the syslog CA certificates are deleted.
switch
```

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

certutil import sshkey

Imports the SSH public key for an SSH user from the remote host using the mentioned login credentials and path name.

Synopsis `certutil import sshkey host remote_ip_address directory ssh_public_key_path user user_acct password password login login_id [rbridge-id {rbridge-id | all}]`
`no certutil sshkey [rbridge-id {rbridge-id | all}]`

Operands

directory <i>path</i>	Specifies the path to the certificate.
file <i>filename</i>	Specifies the SSH public key with a .pub extension.
host <i>remote_ip</i>	Specifies the IP address of the remote host.
login <i>login_id</i>	Specifies the login name in the remote host.
password <i>password</i>	Specifies the password to access the remote host.
rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
<i>rbridge-id</i>	Specifies a unique identifier for a node.
all	Specifies all identifiers for a node.
user <i>user_acct</i>	Specifies the user name to access the remote host.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to import an SSH public key from a remote host for a specified user.

Usage Guidelines Enter `no certutil sshkey user` to delete the SSH public key a specified user.
 The **rbridge-id** operand is supported in VCS mode only.

Examples In Standalone mode

The following command imports a public CA certificate:

```
switch# certutil import sshkey user admin host 10.70.4.106 directory
/users/home40/bmeenaks/.ssh file id_rsa.pub login fvt
Password: *****
switch# 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX6720-60, Event: sshutil,
Status: success, Info: Imported SSH public key from 10.70.4.106 for user 'admin'.
```

The following command deletes the SSH public key for “testuser.”

```
switch# no certutil sshkey user testuser
Do you want to delete the SSH public key file? [y/n]:y
switch# 2012/11/11-13:46:05, [SEC-3050], 3295,, INFO, VDX6720-24, Event: sshutil,
Status: success, Info: Deleted SSH public keys associated to user 'testuser'.
```

In VCS mode

The following command imports a public CA certificate:

```
switch# certutil import sshkey user admin host 10.70.4.106 directory
/users/home40/bmeenaks/.ssh file id_rsa.pub login fvt rbridge-id 3
```

2 certutil import sshkey

```
Password: *****
switch# 2012/11/14-10:28:58, [SEC-3050], 75,, INFO, VDX6720-60, Event: sshutil,
Status: success, Info: Imported SSH public key from 10.70.4.106 for user 'admin'.
```

The following command deletes the SSH public key for “testuser.”

```
switch# no certutil sshkey user testuser rbridge-id 3
Do you want to delete the SSH public key file? [y/n]:y
switch# 2012/11/11-13:46:05, [SEC-3050], 3295,, INFO, VDX6720-24, Event: sshutil,
Status: success, Info: Deleted SSH public keys associated to user 'testuser'.
```

See Also **show cert-util sshkey**

certutil import syslogca

Imports a syslog CA certificate.

Synopsis **certutil import syslogca** *directory path* **file** *filename* **protocol** {*FTP* | *SCP*} **host** *remote_ip* **user** *user_acct* **password** *password* [**rbridge-id** {*rbridge-id* | **all**}]
no certutil syslogca

Operands

directory <i>path</i>	Specifies the path to the certificate.
file <i>filename</i>	Specifies the filename for the certificate.
host <i>remote_ip</i>	Specifies the IP address of the remote host.c
password <i>password</i>	Specifies the password to access the remote host.
protocol <i>FTP</i> <i>SCP</i>	Specifies the protocol used to access the remote server.
rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
<i>rbridge-id</i>	Specifies a unique identifier for a node.
all	Specifies all identifiers for a node.
user <i>user_acct</i>	Specifies the user name to access the remote host.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to import a syslog CA certificate.

Usage Guidelines Enter **no certutil syslogca** to delete the syslog CA certificates of all Active Directory servers.
The **rbridge-id** operand is supported in VCS mode only.

Examples In Standalone mode

The following command imports a syslog CA certificate:

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

The following command deletes a syslog CA certificate:

```
switch# no certutil syslogca
Do you want to delete syslog CA certificate? [y/n]:
```

In VCS mode

The following command imports a syslog CA certificate:

```
switch# certutil import syslogca directory /usr/ldapcacert/ file cacert.pem
protocol SCP host 10.23.24.56 user admin password rbridge-id 3
password:
switch#
```

2 certutil import syslogca

The following command deletes a syslog CA certificate:

```
switch# no certutil syslogca rbridge-id 5  
Do you want to delete syslog CA certificate? [y/n]:
```

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, valid values range from 1 through 64. In Brocade VCS Fabric mode, valid values range 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 The value for **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 through 7 belong to port-channel 1; links 8 through 15 belong to port-channel 2, and links 16 through 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.
- Enter **no channel-group** to remove the port-channel members.

Examples To set the channel-group number to 4 and the mode to *active* on a specific 10-gigabit Ethernet 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 1-gigabit Ethernet interface:

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

2 channel-group

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 this command to toggle the flashing LED locator on the switch. This makes finding the desired 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.

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

Enter **chassis disable** before making configuration changes or running offline diagnostics.

You must execute the **chassis enable** command after running offline diagnostics, or the switch will not boot correctly.

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. Enter **chassis enable** to re-enable the chassis after making configuration changes or running offline diagnostics.

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

You must execute the **chassis enable** command after running offline diagnostics, or the switch will not boot correctly.

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 Global configuration 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 applies to the Brocade VDX 6710, VDX 6720, and VDX 6730.

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

chassis virtual-ip virtual-ipv6

Sets the IPv4 or IPv6 address of a switch chassis.

Synopsis **chassis {virtual-ip | virtual-ipv6}**
no chassis {virtual-ip | virtual-ipv6}

Operands **virtual-ip** Sets an IPv4 address in dotted-decimal notation with a CIDR prefix (mask).
virtual-ipv6 Sets an IPv6 address in colon-separated hexadecimal notation with a CIDR prefix.

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command to change the IPv4 or IPv6 address of a chassis from the default. The default is the initial address of the switch chassis.

Usage Guidelines This is the address that is used to access devices through their RBridge ID. Use this command to change the IP address to facilitate management, for example, if a switch is moved to a different subnet. The IP address of the management platform should be in the same subnet as the devices it manages.

This command applies only to chassis switches, for example, the Brocade VDX 8770.

Use the **no** form of this command to revert to the default address.

Examples IPv4:

```
switch(config)# rbridge-id 4
switch(config-rbridge-id-4)# chassis virtual-ip 10.11.12.13/20
```

IPv6:

```
switch(config)# rbridge-id 4
switch(config-rbridge-id-4)# chassis virtual-ipv6 2001:db8:8086:6502/64
```

See Also **show rbridge-id, show running-config**

cidrecov

Recovers data from Chassis ID cards if possible.

Synopsis **cidrecov**

Operands There are no operands for this command.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command if you receive an error or warning RASLog message that instructs you to run this command.

Two chassis ID (CID) cards contain data necessary for system operation. Each CID contains two Serial Electronically Erasable Programmable Read Only Memory (SEEPR0M) devices. If data on either card becomes corrupt or mismatched, a regularly run CID audit writes messages to the 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 SEEPR0M.

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

Examples Example 1: Noncritical SEEPR0M 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).
```

See Also None

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 There are no restrictions 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, and 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:

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

To configure secure SSH ciphers:

```
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.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

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

Creates a class-map in a policy-map and enters the class-map configuration mode. The class-map must have been created and associated with match criteria using the **class-map** command. (Refer to **qos cos**.)

Synopsis **class** *class-map name*
no class *class-map name*

Operands *class-map name* The designated name for the class-map.

Defaults No created policy-map.

Command Modes Global configuration mode

Description Use this command to configure a class-map for a police policy-map with QoS and policing parameters for inbound or outbound traffic. When you launch the **class** command while in config-policy-map mode (refer to **policy-map**) for a policy, the system is placed in “configure policy-map classification” (config-policy-map-class) mode. Once this is done you can configure QoS and policing parameters for the class-map using the commands for the specific parameters. The commands that set the parameters for a class-map are:

- **cbs**
- **eir**
- **ebs**
- **conform-set-dscp**
- **conform-set-prec**
- **conform-set-tc**
- **exceed-set-dscp**
- **exceed-set-prec**
- **exceed-set-dscp**
- **police cir**
- **set-priority**

Usage Guidelines The QoS and policing parameters define the cir, cbs, ebr, and eir rates and the actions that must occur when traffic conforms or exceeds designated 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.

Enter the **no policy-map name** command 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**).

Enter **no police** while in config-policy-map-class mode to remove all policing parameters for the class-map.

Enter **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 Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples This example configures a class-map called “default” within a policy-map.

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)# class default
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
```

See Also **cbs, conform-set-dscp, conform-set-prec, conform-set-tc, ebs, eir, exceed-set-dscp, exceed-set-prec, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy, set-priority**

class-map

Enters class-map configuration mode.

Synopsis **class-map** *class-map-name*
 no class-map *class-map-name*

Operands *class-map-name* Name of classification map. The map name is restricted to 64 characters.

Defaults The class-name “class-default” is reserved and cannot be created by users.

Command Modes Global configuration mode

Description Use this command to enter class-map configuration mode.

Usage Guidelines Enter **no map class-map** *name* while in global configuration mode to remove the classification map.

Only 128 class maps are allowed.

NOTE

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

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

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

NOTE

The class map created using **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**, **match interface police-priority-map**, **policy-map**, **qos cos**, **service-policy**

clear arp

Clears the ARP statistics cache on the host.

Synopsis **clear arp** [**interface** **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* [*no-refresh*]] | **fortygigabitethernet** *rbridge-id/slot/port* [*no-refresh*]] | [**ip** *ip-address* [*no-refresh*]] | [**no-refresh**] | **ve** *vlan_id* | **vrf** *vrf_name* [**rbridge-id** *rbridge-id*] | **all**]]

Operands

interface Clears the ARP cache for the specified interface only.

gigabitethernet *rbridge-id/slot/port*
Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

no-refresh Deletes the ARP entries.

fortygigabitethernet *rbridge-id/slot/port*
Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

no-refresh Delete the ARP entries.

ip Clears the statistics on all interfaces.

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

no-refresh Delete the ARP entries.

ve *vlan_id* Specifies a VLAN. (Refer to the Usage Guidelines.)

no-refresh Deletes the ARP entries.

vrf *vrf_name* Specifies a VRF instance.

rbridge-id *rbridge-id*
Specifies an RBridge.

all Specifies all RBridges.

Defaults On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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

Clears the IP counter statistics on the switch.

Synopsis `clear counters [access-list {ip | ipv6 | mac} [all] interface {fcoe [vn-number | all] | 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 vlan_id] | storm-control]`

Operands

access-list	Clears the IP counter statistics on all interfaces on the switch.
all	Clears all IP counter statistics on the switch or selected interface.
interface	Specifies the use of the <i>port-channel</i> , <i>gigabitethernet</i> or <i>tengigabitethernet</i> keyword.
port-channel number	Specifies that the interface is a port-channel. The number of available channels range from 1 through 6144.
gigabitethernet rbridge-id/slot/port	Specifies a valid 1-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
tengigabitethernet rbridge-id/slot/port	Specifies a valid 10-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
fortygigabitethernet rbridge-id/slot/port	Specifies a valid 40-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
vlan vlanID	Specifies the VLAN interface to which the ACL is bound.
<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
slot-id	Clears the IP counter statistics on a specified slot in the chassis.
storm-control	Clears counters about traffic controlled by configured rate limits. ve <i>vlan_id</i> Specifies a virtual Ethernet (VE) interface. Refer to Usage Guidelines below.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear the counter statistics on the switch.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also `clear counters access-list`, `clear counters access-list (interface)`, `clear counters access-list (ip)`, `clear counters access-list (MAC)`, `clear counters storm-control`, `clear counters interface`, `clear counters slot-id`, `clear counters (IP)` `clear counters (MAC)`, `clear counters interface`

clear counters access-list

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

Synopsis `clear counters access-list {ip IP_ACL | mac ACL_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 | ve vlan_id | vlan vlan_id} {in | out}`

Operands	ip mac	Specifies the Layer 2 ACL bound to an interface.
	<i>IP_ACL</i>	Name for the access list. A maximum of 63 characters is allowed.
	<i>ACL_NAME</i>	Name for the MAC access list. A maximum of 63 characters is allowed.
	in out	Specifies the binding direction (ingress or egress). In and out parameters are used for access-list ip only.
	interface	Specifies the use of the <i>port-channel</i> , <i>fibrechannel</i> , <i>gigabitethernet</i> or <i>tengigabitethernet</i> keyword.
	port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	ve <i>vlan_id</i>	Specifies the virtual Ethernet interface to which the ACL is bound. (Refer to the Usage Guidelines).
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	vlan <i>vlan_id</i>	Specifies the VLAN interface to which the ACL is bound. (Refer to the Usage Guidelines).

	<i>rbridge-id</i> Specifies the RBridge ID. This is not valid in standalone mode. <i>slot</i> Specifies a valid slot number. <i>port</i> Specifies a valid port number.
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 such as LLDP, LACP, MSTP, and so on. For Brocade VDX switches, the slot number is always 0 (zero). On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
Examples	To clear the statistics for the 10-gigabit Ethernet interface 5/0/1: <pre>switch# clear counters interface tengigabitethernet 5/0/1</pre> To clear the statistics for all the interfaces on the linecard in slot 0 (zero): <pre>switch# clear counters slot-id 0</pre>
See Also	clear counters access-list (interface) , clear counters access-list (ip) , clear counters access-list (MAC) ,

clear counters access-list (interface)

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

Synopsis `clear counters access-list interface {port-channel number | gigabitethernet rbridge-id/slot/port | tengigabitethernet rbridge-id/slot/port | fortygigabitethernet rbridge-id/slot/port} | ve vlan_id | vlan vlan_id | port-channel number} {in | out}`

Operands	interface	Specifies the use of the <i>port-channel</i> , <i>gigabitethernet</i> or <i>tengigabitethernet</i> keyword.
	port-channel <i>number</i>	Specifies that the interface is a port-channel. The number of available channels range from 1 through 6144.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	ve <i>vlan_id</i>	Specifies the virtual Ethernet interface to which the ACL is bound. (Refer to the Usage Guidelines.)
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	vlan <i>vlanID</i>	Specifies the VLAN interface to which the ACL is bound.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
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 such as LLDP, LACP, MSTP, and so on.

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

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples To clear the statistics for the 10-gigabit 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 statistics access-list**

clear counters access-list (ip)

Clears the IP ACL counters for all interfaces that have ACL applied on them or for a specific interface.

Synopsis **clear counters access-list ip** *IP_ACL*
 [**interface** [**port-channel** *number* | **fortygigabitethernet** *rbridge-id/slot/port* |
 gigabitethernet *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port*]] [**in** | **out** | **interface**]
 clear counters {**all** | **access-list ip** *IP_ACL* | **interface** {**port-channel** *number* |
 gigabitethernet *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* |
 fortygigabitethernet *rbridge-id/slot/port*} | **slot-id** *number* | **ve** *vlan_id*} {**in** | **out**}

Operands	<i>IP ACL</i>	Specifies the name of the IP ACL. A maximum of 63 characters is allowed.
	in out	Specifies the binding direction (ingress or egress). In and out parameters are used for access-list ip only.
	interface	Specifies the use of the <i>port-channel</i> , <i>fortygigabitethernet</i> , <i>gigabitethernet</i> , <i>tengigabitethernet</i> , or <i>vlan</i> keyword.
	port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	in	Specifies the ingress direction.
	interface	Specifies the interface.
	out	Specifies the egress direction.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	in	Specifies the ingress direction.
	interface	Specifies the interface.
	out	Specifies the egress direction.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	in	Specifies the ingress direction.

interface	Specifies the interface.
out	Specifies the egress direction.
ve vlan_id	Specifies the virtual Ethernet interface to which the ACL is bound. (Refer to the Usage Guidelines.)
rbridge-id	Specifies the RBridge ID. 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 IP 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.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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

```
switch# clear counters access-list ip test interface tengigabitethernet 0/1
```

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

```
switch# clear counters access-list ip test
```

See Also [show statistics access-list](#)

clear counters access-list (MAC)

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

Synopsis `clear counters access-list mac name [interface [port-channel number | fortygigabitethernet rbridge-id/slot/port | gigabitethernet rbridge-id/slot/port | tengigabitethernet rbridge-id/slot/port | vlan vlan_id]] [in | out | interface]`

Operands	<i>MAC ACL name</i>	Specifies the name of the MAC ACL. A maximum of 63 characters is allowed.
	interface	Specifies the use of the <i>port-channel</i> , <i>tengigabitethernet</i> , or <i>vlan</i> keyword.
	port-channel number	Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.
	fortygigabitethernet rbridge-id/slot/port	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	in	Specifies the ingress direction.
	interface	Specifies the interface.
	out	Specifies the egress direction.
	gigabitethernet rbridge-id/slot/port	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	vlan vlan_id	Specifies a VLAN. (Refer to the Usage Guidelines.)
	in	Specifies the ingress direction.
	interface	Specifies the interface.
	out	Specifies the egress direction.
	tengigabitethernet rbridge-id/slot/port	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	in	Specifies the ingress direction.
	interface	Specifies the interface.
	out	Specifies the egress direction.

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. On the Brocade VDX family of hardware, switches, 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
Examples	To clear counters for the configured MAC access list named test on an interface: <pre>switch# clear counters access-list mac test interface tengigabitethernet 0/1</pre> To clear counters for the configured MAC access list named test on all interfaces on which this ACL is applied: <pre>switch# clear counters access-list mac test</pre>
See Also	show mac-address-table, show statistics access-list

clear counters interface

Clears the IP counter statistics on a specified interface on the switch.

Synopsis	clear counters interface { <i>fcoe</i> { <i>vn-number/rbridge-id/port</i> <i>all</i> } <i>fibrechannel</i> { <i>rbridge-id/slot/port</i> } port-channel <i>number</i> [<i>fortygigabitethernet</i> { <i>rbridge-id/slot/port</i> <i>all</i> } <i>gigabitethernet</i> { <i>rbridge-id/slot/port</i> } <i>tengigabitethernet</i> { <i>rbridge-id/slot/port</i> } <i>vlan</i> { <i>vlan_id</i> }}	
Operands	interface	Specifies the use of the <i>fcoe</i> , <i>port-channel</i> , <i>fibrechannel</i> , <i>fortygigabitethernet</i> , <i>gigabitethernet</i> , <i>tengigabitethernet</i> , or <i>vlan</i> keyword.
	fcoe <i>vn-number/rbridge-id/port</i>	
		Specifies the FCOE interface name.
	<i>vn-number</i>	Specifies the VN number for FCoE.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>port</i>	Specifies a valid port number.
	all	Clears counters for all FCOE interfaces.
	fibrechannel <i>rbridge-id/slot/port</i>	
		Specifies a valid Fibre Channel interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	
		Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet <i>rbridge-id/slot/port</i>	
		Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	
		Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	port-channel <i>number</i>	
		Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

vlan *vlan_id* Specifies a VLAN interface. (Refer to the Usage Guidelines.)

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 such as LLDP, LACP, MSTP, and so on.

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

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also None

clear counters slot-id

Clears the IP counter statistics on a specified slot in the chassis.

Synopsis `clear counters slot-id num`

Operands *num* Specifies a valid integer.

Defaults None

Command Modes Privileged EXEC mode

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

Usage Guidelines The **clear counters all** command does not clear counters for any of the protocol daemon stats such as LLDP, LACP, MSTP, and so on.

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

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* | **fibrenchannel** {*rbridge-id/slot/port*} | **gigabitethernet** {*rbridge-id/slot/port*} | **tengigabitethernet** {*rbridge-id/slot/port*} | **fortygigabitethernet** {*rbridge-id/slot/port*} | **slot-id** *number* | **ve** *vlan_id*} {**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.

in | out Specifies the binding direction (ingress or egress). In and out parameters are used for access-list ip only.

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

port-channel *number*
Specifies the interface is a port-channel. The number of available channels range from 1 through 6144.

fibrenchannel *rbridge-id/slot/port*
Specifies a valid Fibre Channel interface.

rbridge-id Specifies the RBridge ID. This 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-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

fortygigabitethernet *rbridge-id/slot/port*
Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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.

2 clear counters (IP)

ve <i>vlan_id</i>	Specifies the virtual Ethernet (VE) interface to which the ACL is bound. (Refer to the Usage Guidelines.)
rbridge-id	Specifies RBridge ID for node-specific ACL interface details.
<i>rbridge-id</i> all	Specifies the unique identifier for a switch. All refers to all rbridge-ids in the cluster.

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).

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples To clear the statistics for the 10-gigabit 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 igmp groups**

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*) | **fibrenchannel** {*rbridge-id/slot/port*} | **gigabitethernet** {*rbridge-id/slot/port*} | **tengigabitethernet** {*rbridge-id/slot/port*} | **fortygigabitethernet** {*rbridge-id/slot/port*} | **slot-id** *number* | **vlan** *vlan_id*}

Operands **all** Specifies to clear statistics on all interfaces.

access-list mac *access_list_name* Specifies the name of the MAC access list.

in | out Specifies the binding direction (ingress or egress). In and out parameters are used for access-list ip only.

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

port-channel *number* Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.

fibrenchannel *rbridge-id/slot/port* Specifies a valid Fibre Channel interface.

rbridge-id Specifies the RBridge ID. This 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-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port* Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

fortygigabitethernet *rbridge-id/slot/port* Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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 interface to which the ACL is bound. (Refer to the Usage Guidelines.)

2 clear counters (MAC)

	slot-id <i>number</i>	Specifies the slot number of the linecard.
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). On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.	
Examples	To clear the statistics for the 10-gigabit Ethernet interface 5/0/1: <pre>switch# clear counters interface tengigabitethernet 5/0/1</pre> To clear the statistics for all the interfaces on the linecard in slot 0 (zero): <pre>switch# clear counters slot-id 0</pre>	
See Also	show ip igmp groups	

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} rbridge-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 (Broadcast, Unknown unicast and Multicast)-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 parameter to clear counters on a per-port basis.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear 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 10-gigabit Ethernet 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 10-gigabit Ethernet interface 102/4/1:

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

2 clear counters storm-control

To clear counters for all multicast traffic in the system:

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

To clear all BUM-related counters in the system:

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

See Also None

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** *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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 [rbridge-id rbridge-id]`

`clear edge-loop-detection interface {fortygigabitethernet {rbridge-id/slot/port} | gigabitethernet {rbridge-id/slot/port} | tengigabitethernet {rbridge-id/slot/port} | port-channel num}`

Operands	<code>rbridge-id</code>	A unique identifier for the switch. Values are from 1 through 239.
	<code>fortygigabitethernet rbridge-id/slot/port</code>	Specifies a valid 1-gigabit Ethernet interface.
	<code>rbridge-id</code>	Specifies the RBridge ID. This is not valid in standalone mode.
	<code>slot</code>	Specifies a valid slot number.
	<code>port</code>	Specifies a valid port number.
	<code>gigabitethernet rbridge-id/slot/port</code>	Specifies a valid 1-gigabit Ethernet interface.
	<code>rbridge-id</code>	Specifies the RBridge ID. This is not valid in standalone mode.
	<code>slot</code>	Specifies a valid slot number.
	<code>port</code>	Specifies a valid port number.
	<code>tengigabitethernet rbridge-id/slot/port</code>	Specifies a valid 10-gigabit Ethernet interface.
	<code>rbridge-id</code>	Specifies the RBridge ID. This is not valid in standalone mode.
	<code>slot</code>	Specifies a valid slot number.
	<code>port</code>	Specifies a valid port number.
	<code>port-channel number</code>	Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
		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 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.
		If the rbridge-id is specified, it clears edge-loop-detection from the specific node. Otherwise, it clears edge-loop-detection from all nodes in the VCS cluster.

2 clear edge-loop-detection

Examples 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 vn-number/rbridge-id/front-port-number] | [vlan vlan_id] | [interface tengigabitethernet rbridge-id/slot/port] | [vfid vfid] | [device device-wwn]`

Operands

`interface fcoe vn-number/rbridge-id/front-port-number`
The VN number/RBridge ID/front-port number for the virtual-fabric.

`vlan vlan_id`
The VLAN ID for the device. (Refer to the Usage Guidelines.)

`interface tengigabitethernet rbridge-id/slot/port`
Specifies a valid 10-gigabit Ethernet interface.

`rbridge-id`
Specifies the RBridge ID. 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 Use this command to clear the FCoE login for a given FCoE interface, VLAN, VFID, or device WWN.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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

2 clear ip bgp dampening

clear ip bgp dampening

Reactivates all suppressed BGP4 routes.

Synopsis **clear ip bgp dampening** [*ip-addr* [/*mask*]]

Operands *ip-addr* IPv4 address of a specified route in dotted-decimal notation.
 mask (Optional) IPv4 mask of a specified route in CIDR notation.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to unsuppress all suppressed BGP4 routes.

Usage Guidelines None

Examples To unsuppress all suppressed BGP4 routes:

```
switch# clear ip bgp dampening
```

See Also None

clear ip bgp flap-statistics

Clears the dampening statistics for a BGP4 route without changing the dampening status of the route.

Synopsis **clear ip bgp flap-statistics** [*ip-addr* {/mask} | **neighbor** *ip-addr* | **regular-expression** *string*]

Operands	<i>ip-addr</i>	IPv4 address of a specified route in dotted-decimal notation.
	<i>mask</i>	(Optional) IPv4 mask of a specified route in CIDR notation.
	neighbor	Clears dampening statistics only for routes learned from the specified neighbor.
	<i>ip-addr</i>	IPv4 address of the neighbor.
	regular-expression	Specifies a regular expression.
	<i>string</i>	Regular expression.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear the dampening statistics for a BGP4 route without changing the dampening status of the route.

Usage Guidelines None

Examples To clear the dampening statistics for a BGP4 route:

```
switch# clear ip bgp flap-statistics 10.0.0.0/16
```

See Also None

2 clear ip bgp local routes

clear ip bgp local routes

Clears all BGP4 local routes from the IP route table and resets the routes.

Synopsis **clear ip bgp local routes**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear all BGP4 local routes from the IP route table and reset the routes.

Usage Guidelines None

Examples To clear all BGP4 local routes:

switch# **clear ip bgp local routes**

See Also None

clear ip bgp neighbor

Requests a dynamic refresh of BGP4 connections or routes from a neighbor, with a variety of options.

Synopsis `clear ip bgp neighbor` [*all* | *as-num* | *peer-group-name* | *ip-addr*] [*last-packet-with-error* | *notification-errors* | *soft* [*in* | *out*] | *soft-outbound* | *traffic*] [*rbridge-id* *rbridge-id*]

Operands	all	Resets and clears all BGP4 connections to all neighbors.
	<i>as-num</i>	Clears all BGP4 connections within this autonomous system. Range is from 1 through 4294967295.
	<i>peer-group-name</i>	Clears all BGP4 connections in this peer group. Range is from 1 through 63 characters.
	<i>ip-addr</i>	Clears all BGP4 connections with this IPv4 address, in dotted-decimal notation.
	last-packet-with-error	Clears all BGP4 connections identified as having the last packet received with an error.
	notification-errors	Clears all BGP4 connections identified as having notification errors.
	soft	Refreshes routes received from or sent to the neighbor.
	in	Refreshes received routes.
	out	Refreshes sent routes.
	soft-outbound	Refreshes all outbound routes by applying new or changed filters, but sends only the existing routes affected by the new or changed filters to the neighbor.

NOTE

Use **soft-outbound** only if the outbound policy is changed. This operand updates all outbound routes by applying the new or changed filters. However, the device sends to the neighbor only the existing routes that are affected by the new or changed filters. The **soft out** operand updates all outbound routes and then sends the entire BGP4 route table on the device to the neighbor after the device changes or excludes the routes affected by the filters.

traffic Clears the counters (resets them to 0) for BGP4 messages.

rbridge-id *rbridge-id* Selects an RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to request a dynamic refresh of BGP4 connections or routes from a neighbor, with a variety of options.

Usage Guidelines None

Examples To refresh all BGP4 neighbor connections:

```
switch# clear ip bgp neighbor all
```

See Also None

2 clear ip bgp routes

clear ip bgp routes

Clears BGP4 routes from the IP route table and resets the routes.

Synopsis **clear ip bgp routes** [*ip-addr* [/*mask*]]

Operands *ip-addr* IPv4 address of a specified route in dotted-decimal notation.
 mask (Optional) IPv4 mask of a specified route in CIDR notation.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear BGP4 routes from the IP route table and reset the routes.

Usage Guidelines None

Examples To clear BGP4 routes:

 switch# **clear ip bgp routes 10.0.0.0/16**

See Also None

clear ip bgp traffic

Clears the BGP4 message counter for all neighbors.

Synopsis **clear ip bgp traffic**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear the BGP4 message counters (resetting them to 0) for all neighbors.

Usage Guidelines None

Examples To clear the BGP4 message counters:

 switch# **clear ip bgp traffic**

See Also None

clear ip dhcp relay statistics

Clears IP DHCP Relay statistics

Synopsis `clear ip dhcp relay statistics` [**ip-address** *ip-address*] [**rbridge-id** *rbridge-id* | **all** | **range**]

Operands **ip-address** *ip-addr* IPv4 address of DHCP server where client requests are to be forwarded.
rbridge-id *rbridge-id* Specific RBridge identification. You can specify multiple RBridge IDs, separated by commas.

all All RBridge IDs in the logical chassis cluster.

range A range of RBridge IDs separated by a dash or commas, for example:
 1-3 - RBridge ID 1 through 3
 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5
 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Defaults If the **rbridge-id** parameter is omitted, statistics clear for the local switch. If the **ip_address** parameter is omitted, statistics clear for all configured addresses on defined switches.

Command Modes Privileged EXEC mode

Description Clears IP DHCP Relay statistics for a specific IP DHCP Relay address or all addresses on a local switch, specific switches, or all nodes in a logical chassis cluster.

Usage Guidelines No spaces are allowed in the range string. The range does not need to be contiguous (for example, 1-2,5). You can also specify **all** for all RBridge IDs in a logical chassis cluster.

Examples Clear statistics for IP DHCP Relay addresses on RBridge IDs 1, 3, and 5.

```
switch# clear ip dhcp relay statistics rbridge-id 1,3,5
```

Clear statistics for IP DHCP Relay address 10.1.0.1 configured on RBridge IDs 1, 3, and 5.

```
switch# clear ip dhcp relay statistics ip-address 10.1.0.1 rbridge-id 1,3,5
```

See Also `show ip dhcp relay statistics`

clear ip igmp groups

Clears information related to learned groups in the IGMP 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* | **ve** *vlan_id* [**rbridge** *rbridge-id*] | **rbridge** *rbridge-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 *rbridge-id/slot/port*

Specifies a valid external 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

interface gigabitethernet *rbridge-id/slot/port*

Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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 number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.

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

ve *vlan_id* Specifies groups on the specified virtual Ethernet (VE) interface. (Refer to the Usage Guidelines.)

rbridge *rbridge-id* Specifies an RBridge.

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.

2 clear ip igmp groups

Usage Guidelines	On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
Examples	To clear information for all groups in the IGMP protocol: <pre>switch# clear ip igmp groups</pre>
See Also	None

clear ip igmp statistics interface

Clears statistical information related to the IGMP module.

Synopsis **clear ip igmp statistics interface** {**fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number* | **tengigabitethernet** *rbridge-id/slot/port* | **ve** *vlan_id* | **vlan** *vlan_id* [**rbridge** *rbridge-id*] | **rbridge** *rbridge-id*}

Operands **fortygigabitethernet** *rbridge-id/slot/port*
Clears counters on the specified, valid 40 Gbps port interface.

rbridge-id Specifies the RBridge ID.
This parameter 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-gigabit Ethernet interface

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

loopback *number* Specifies a loopback port number in the range of 1 to 255.

port-channel *number*
Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.

tengigabitethernet *rbridge-id/slot/port*
Clears counters on the specified, valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

ve *vlan_id* Specifies a virtual Ethernet (VE) interface. (Refer to the Usage Guidelines.)

vlan *vlan_id* Specifies a VLAN interface. (Refer to the Usage Guidelines.)

rbridge *rbridge-id* Specifies an RBridge.

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 switches, 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). Valid VLAN IDs are as follows:

2 clear ip igmp statistics interface

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

In logical chassis mode:

- When the **rbridge-id** option is specified, details for the ve interface on that particular rbridge are cleared.
- If **rbridge-id** is not specified, details for the ve interface on the node on which the command is executed are cleared.
- When **rbridge-id all** is specified, all ve interfaces with that **rbridge-id** from all the nodes in the cluster are cleared.

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* | **loopback** *number* | **port-channel** *number* | **tengigabitethernet** *rbridge-id/slot/port* | **ve** *vlan_id*} [**vrf** *name* [**rbridge** *rbridge-id*]] | [**rbridge-id** *rbridge-id*]

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 <i>rbridge-id/slot/port</i>	Clears counters on the specified, valid 40 Gbps port interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This parameter is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Clears counters on the specified, valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	loopback <i>number</i>	Specifies a loopback port number in the range of 1 to 255.
	port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Clears counters on the specified, valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	ve <i>vlan_id</i>	Specifies a virtual Ethernet (VE) interface. (Refer to the Usage Guidelines.)
	rbridge <i>rbridge-id</i>	Clears the specified RBridge.
	vrf <i>name</i>	Clears the specified VRF.
	neighbor	Clears the specified neighbor, or clears all neighbors.

2 clear ip ospf

<i>A.B.C.D</i>	Specifies the IP address of the neighbor to clear.
all	Clears all neighbors.
routes	Clears matching routes or clears all routes.
<i>A.B.C.D</i>	Clears all routes that match the prefix and mask that you specify.
all	Clears all routes.

Defaults None

Command Modes Privileged EXEC mode

Usage Guidelines If the physical interface type and name are specified, the **rbridge-id** *rbridge-id* option is not available.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples To restart the OSPF processes:

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

See Also None

clear ip pim mcache

Clears the Protocol Independent Multicast forwarding cache.

Synopsis **clear ip pim mcache** [*IP-addr* [*IP-addr*]]

Operands *IP-addr* Group or source IPv4 address. One or two IP addresses (Unicast or Multicast) can be specified.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear the Protocol Independent Multicast forwarding cache.

Usage Guidelines None

Examples None

See Also **clear ip pim rp-map, clear ip pim traffic**

2 clear ip pim rp-map

clear ip pim rp-map

Clears the static multicast forwarding table.

Synopsis clear ip pim rp-map

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear the static multicast forwarding table.

Usage Guidelines This command should be used after the static Rendezvous Point configuration has been changed. This allows Protocol Independent Multicast to immediately start using the new Rendezvous Point, rather than waiting for the old information to expire.

Examples None

See Also clear ip pim mcache, clear ip pim traffic

clear ip pim traffic

Clears the Protocol Independent Multicast (PIM) traffic counters.

Synopsis **clear ip pim traffic**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description This command clears the Protocol Independent Multicast (PIM) traffic counters.

Usage Guidelines None

Examples None

See Also **clear ip pim rp-map, clear ip pim mcache**

clear ip route

Clears IP routes.

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

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.
vrf *name* Clears the specified VRF.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear either a specified route or all IP routes in the IP routing tables.

Usage Guidelines None

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

switch# **clear ip route 192.158.1.1/24**

See Also None

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. Valid values range from 1 through 64 in standalone mode and 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**

2 clear 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**

clear lldp neighbors

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

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

Operands **interface** Use this parameter followed by the slot or port number to identify the interface.

fortygigabitethernet *rbridge-id/slot/port*

Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*

Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This 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-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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** parameter is not specified, this command clears the LLDP neighbor information received on all the interfaces.

Examples To clear the LLDP neighbor 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** [**fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands **interface** Use this parameter followed by the slot or port number to identify the interface.

fortygigabitethernet *rbridge-id/slot/port*

Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*

Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This 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-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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** parameter 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 RBridge ID. This parameter 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**, **log-dampening-debug (BGP)**, **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	Enables RBridge ID mode to support VCS on individual nodes.
<i>rbridge-id</i>	Specifies a unique identifier for a node.
all	Specifies all identifiers for a node.

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.
The **rbridge-id** operand is supported in VCS mode only.
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 SYSTEM messages on the local switch:

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

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

clear mac-address-table dynamic

Provides a mechanism for clearing the MAC interface status and configuration information.

Synopsis `clear mac-address-table dynamic [address mac_address | interface fortygigabitethernet rbridge-id/slot/port | interface tengigabitethernet rbridge-id/slot/port | interface gigabitethernet rbridge-id/slot/port | vlan vlan_id]`

Operands `address mac_address` MACaddress in HHHH.HHHH.HHHH format.

`interface` Use this parameter followed by the slot or port number to identify the interface.

`fortygigabitethernet rbridge-id/slot/port` Specifies a valid 40-gigabit Ethernet interface.

`rbridge-id` Specifies the RBridge ID. This is not valid in standalone mode.

`slot` Specifies a valid slot number.

`port` Specifies a valid port number.

`tengigabitethernet rbridge-id/slot/port` Specifies a valid 10-gigabit Ethernet interface.

`rbridge-id` Specifies the RBridge ID. This 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-gigabit Ethernet interface.

`rbridge-id` Specifies the RBridge ID. This is not valid in standalone mode.

`slot` Specifies a valid slot number.

`port` Specifies a valid port number.

`vlan vlan_id` Specifies a VLAN interface.

Defaults None

Command Modes Privileged EXEC mode

Description Provides a mechanism for clearing the MAC interface status and configuration information.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

2 clear mac-address-table dynamic

Examples None

See Also None

clear nas statistics

Clears automatic network attached storage (NAS) statistics.

Synopsis **clear nas statistics all** | **server-ip** *ip_addr/prefix* [**vlan** *vlan_id* | **vrf** *VRF_name*] [**rbridge-id** *rbridge-id*]

Operands

all	Shows all gathered statistics.
server-ip	IP address for which to clear Auto-NAS statistics.
<i>ip_addr/prefix</i>	IPv4 address/prefix of a specified Auto-NAS port.
vlan <i>VLAN_id</i>	Specifies a VLAN interface for which to clear the statistics.
vrf <i>VRF_name</i>	Specifies an OSPF VRF interface for which to clear the statistics.
[rbridge-id <i>rbridge-id</i>]	Specifies an RBridge ID for which to clear the statistics.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear the specified Auto-NAS statistics.

Usage Guidelines This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Examples switch# **clear nas statistics all server-ip 1.1.1.0/24**

See Also **nas auto-qos, nas server-ip, show nas statistics, show running-config nas server-ip, show system internal nas, show cee maps**

clear overlay-gateway

Clear counters for the specified gateway.

Synopsis **clear overlay-gateway** *name* { **statistics** | **vlan statistics** }

Operands *name* Specifies the name of the VXLAN gateway profile.
 statistics Clears all statistics for the VXLAN gateway.
 vlan statistics Clears per-VLAN statistics for the VXLAN gateway.

Defaults None

Command Modes Privileged EXEC mode

Description} Clears all counters for the specified VXLAN gateway for all tunnels on all RBridges.

Usage Guidelines This command is available only for a switch that is in logical chassis cluster mode.
 If you specify the VXLAN gateway name, the gateway must already be configured.
 If you specify VLAN IDs, these VLANS must already be configured as exported VLANs for the gateway.

Examples To clear all counters for the already configured VXLAN gateway named *gateway1*:
 sw0# **clear overlay-gateway gateway1 statistics**

See Also

clear policy-map-counters

Provides a mechanism for clearing the policy map counters.

Synopsis `clear policy-map-counters [interface fortygigabitethernet rbridge-id/slot/port | interface tengigabitethernet rbridge-id/slot/port | interface gigabitethernet rbridge-id/slot/port | port-channel number]`

Operands	interface	Use this parameter followed by the slot or port number to identify the interface.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
Defaults	None	
Command Modes	Privileged EXEC	
Description	Provides a mechanism for clearing the policy map counters.	
Usage Guidelines	None	
Examples	None	
See Also	None	

clear sessions

To log out the user sessions connected to the switch.

Synopsis **clear sessions** [**rbridge-id** *rbridge-id* | **all**]

Operands	rbridge-id	Enables RBridge ID mode to support VCS on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
	all	Specifies all identifiers for a node.

Defaults None

Command Modes Privileged EXEC

Description Logs out the user sessions connected to the switch.

Usage Guidelines This command is not distributed across the cluster. The RBridge ID of the node should be used to log out users connected to the individual nodes.

The **rbridge-id** operand is supported in VCS mode only.

Examples Standalone mode

```
switch# clear sessions
This operation will logout all the user sessions. Do you want to continue
(yes/no)?: y
```

VCS mode

```
switch# clear sessions rbridge-id 3
This operation will logout all the user sessions. Do you want to continue
(yes/no)?: y
```

See Also None

clear sflow statistics

Clears all sFlow statistics.

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

Operands **interface** Use this parameter followed by the slot or port number to identify the interface.

fortygigabitethernet *rbridge-id/slot/port* -

Specifies a valid 40-gigabit Ethernet interface.

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

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*

Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the routing bridge ID. This 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-gigabit Ethernet interface.

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

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults This command has no defaults.

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 |
fortygigabitethernet rbridge-id/slot/port | tengigabitethernet rbridge-id/slot/port |
gigabitethernet rbridge-id/slot/port]`

Operands

interface	Specifies the interface on which to clear the spanning-tree counters.
port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	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** parameter is not specified, spanning-tree counters are cleared for all interfaces. If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Examples

To clear spanning-tree counters for all interfaces:

```
switch# clear spanning-tree counter
```

To clear spanning-tree counters for a 10-gigabit 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 spanning-tree detected-protocols

Clears all spanning-tree detected protocols on the interface.

Synopsis `clear spanning-tree detected-protocols [interface | port-channel number | fortygigabitethernet rbridge-id/slot/port | tengigabitethernet rbridge-id/slot/port | gigabitethernet rbridge-id/slot/port]`

Operands

interface	Specifies the interface on which to clear the spanning-tree counters.
port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear the detected protocols on the interface.

Usage Guidelines If the **interface** parameter is not specified, spanning-tree detected protocols are cleared for all interfaces.

Examples

To clear detected protocols for all interfaces:

```
switch# clear spanning-tree detected-protocols
```

To clear detected protocols for a 10-gigabit Ethernet interface:

```
switch# clear spanning-tree detected-protocols interface tengigabitethernet 0/1
```

To clear detected protocols for port-channel 23:

```
switch# clear spanning-tree detected-protocols 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	Enables RBridge ID mode to support VCS on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
	all	Specifies all identifiers for a node.

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.
The **rbridge-id** operand is supported in VCS mode only.

Examples To remove core files from the local switch:

```
switch# clear support
```

See Also **copy support**, **show support**

clear udd statistics

Clears UDLD statistics.

Synopsis `clear udd statistics [interface {fortygigabitethernet rbridge-id/slot/port | gigabitethernet rbridge-id/slot/port | tengigabitethernet rbridge-id/slot/port}]`

Operands **fortygigabitethernet** *rbridge-id/slot/port*
 Specifies a valid 40-gigabit Ethernet interface for clearing UDLD statistics.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface clearing UDLD statistics.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface clearing UDLD statistics.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Clears either all unidirectional link detection (UDLD) protocol statistics or clears the statistics on a specified port.

Usage Guidelines None

Examples To clear UDLD statistics on a specific tengigabitethernet interface:

```
switch# clear udd statistics interface te 5/0/1
```

See Also protocol udd, show udd, udd enable

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*}] [**ve** *vlan*]

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

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

fortygigabitethernet *rbridge-id/slot/port*

 Specifies a valid 40-gigabit Ethernet port interface.

rbridge-id Specifies the RBridge ID.

 This parameter 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-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*

 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

ve *vlan* Specifies the VE vlan number.

session *VRID* Specifies the virtual group ID on which to clear statistics. Valid values range from 1 through 128.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to clear VRRP session statistics for all virtual groups, for a specified interface or for a specified virtual group.

Usage Guidelines This command is for VRRP and VRRP-E. VRRP-E supports only the **ve** interface type.
To clear all statistics, use the **clear vrrp statistics** command with no operands.

Examples To clear all VRRP statistics for all virtual groups:

```
switch# clear vrrp statistics
```

To clear statistics for a 10-gigabit Ethernet 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
```

See Also None

client-to-client-reflection (BGP)

Enables routes from one client to be reflected to other clients by the host device on which it is configured.

Synopsis **client-to-client-reflection**
no client-to-client-reflection

Operands None

Defaults This feature is enabled.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to enable routes from one client to be reflected to other clients. The host device on which it is configured becomes the route-reflector server.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To configure client-to-client reflection on the host device:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# client-to-client-reflection
```

See Also None

clock set

Sets the local clock date and time.

Synopsis `clock set CCYY-MM-DDTHH:MM:SS [rbridge-id {rbridge-id | all}]`

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.

rbridge-id Enables RBridge ID mode to support logical chassis cluster mode on individual nodes.

rbridge-id Specifies a unique identifier for a node.

all Specifies all identifiers for a node.

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 if you are in Standalone mode. This command is not distributed across a cluster. The RBridge ID of the node should be used to set the clock.

The **rbridge-id** parameter is supported in Logical chassis cluster mode only.

Examples To set the date and time to March 17, 2010, 15 minutes past noon in Standalone mode or on an individual node:

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

To set the date and time to March 17, 2010, 15 minutes past noon in Logical chassis cluster mode for all switches in the cluster:

```
switch# clock set rbridge-id all 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* [**rbridge-id** {*rbridge-id* | **all**}]
no clock timezone [**rbridge-id** *rbridge-id*]

Operands *region* Specifies the region's time zone.
 city Specifies the city's time zone.
 rbridge-id Enables RBridge ID mode to support Logical chassis cluster mode on individual nodes.
 rbridge-id Specifies a unique identifier for a node.
 all Specifies all identifiers for a node.

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. When using the **no** operand, you do not need to reference a timezone setting.

The **no** operand is not distributed across the cluster. The RBridge ID of the node should be used.

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 might need to reset the time zone information.

The **rbridge-id** operand is supported in VCS mode only.

Examples Standalone mode

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

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

To remove the timezone setting:

```
switch# no clock timezone
```

Logical chassis cluster mode

To set the time zone to Pacific Standard Time in North America on all nodes in the cluster:

```
switch# clock timezone America/Los_Angeles rbridge-id all
```

To remove the timezone setting:

```
switch# no clock timezone rbridge-id 5
```

See Also clock set, ntp server, show clock

cluster-id (BGP)

Configures a cluster ID for the route reflector.

Synopsis **cluster-id** [*num* | **ipv4-address** *ip-addr*]
no cluster-id

Operands *num* Integer value for cluster ID. Range is from 1 through 65535.
 ip-addr IPv4 address in dotted-decimal notation.

Defaults The default cluster ID is the device ID.

Command Modes BGP configuration mode

Description Use this command to configure a cluster ID for the route reflector. When configuring multiple route reflectors in a cluster, use the same cluster ID to avoid loops within the cluster.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To configure a cluster ID for the route reflector:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# cluster-id 1234
```

See Also None

compare-med-empty-aspath (BGP)

Enables comparison of Multi-Exit Discriminators (MEDs) for internal routes that originate within the local autonomous system (AS) or confederation.

Synopsis **compare-med-empty-aspath**
 no compare-med-empty-aspath

Operands None

Defaults None

Command Modes BGP configuration mode

Description Use this command to enable the comparison of MEDs for internal routes that originate within the local AS or confederation.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To configure the device to compare MEDs:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# compare-med-empty-aspath
```

See Also None

compare-routerid (BGP)

Enables comparison of router IDs, so that the path-comparison algorithm compares the device IDs of neighbors that sent otherwise equal-length paths.

Synopsis	compare-routerid no compare-routerid
Operands	None
Defaults	None
Command Modes	BGP configuration mode
Description	Use this command to enable the comparison of the router IDs of otherwise equal paths.
Usage Guidelines	Use the no form of this command to restore the default.
Examples	To configure the device always to compare router IDs: <pre>switch(config)# rbridge-id 10 switch(config-rbridge-id-10)# router bgp switch(config-bgp-router)# compare-routerid</pre>
See Also	None

configure terminal

Enters global configuration mode.

Synopsis **configure terminal**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Descriptions Use this command to enter global configuration mode.

Usage Guidelines None

Examples None

See Also **exit**

conform-set-dscp

Optional command for configuring the packet DSCP priority of a class-map.

Synopsis **conform-set-dscp** *dscp-num*
no conform-set-dscp *dscp-num*

Operands *dscp-num* Specifies that traffic with bandwidth requirements within the rate configured for CIR that has the packet DSCP priority set to the value specified by the *dscp-num* variable. Valid values are 0 through 63.

Defaults None

Command Modes Policy-map class police configuration mode

Description This command configures the packet DSCP priority of a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples Example of setting this parameter.

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# conform-set-dscp 3
```

See Also **cbs**, **conform-set-prec**, **conform-set-tc**, **ebs**, **eir**, **exceed-set-dscp**, **exceed-set-prec**, **exceed-set-tc**, **police cir**, **police-priority-map**, **policy-map**, **qos cos**, **service-policy**, **set-priority**

conform-set-prec

Optional command for configuring the packet IP precedence value of a class-map.

Synopsis **conform-set-prec** *prec-num*

no conform-set-prec *prec-num*

Operands *prec-num* 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. Valid values are 0 through 7.

Defaults None

Command Modes Policy-map class police configuration mode

Description This command configures the packet IP precedence value of a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples Example of setting this parameter.

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# conform-set-prec 3
```

See Also **cbs, conform-set-dscp, conform-set-tc, ebs, eir, exceed-set-dscp, exceed-set-prec, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy, set-priority**

conform-set-tc

Optional command for configuring the CIR internal queue assignment of a class-map.

Synopsis **conform-set-tc** *trafficclass*
 no conform-set-tc *trafficclass*

Operands *trafficclass* 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. Valid values are 0 through 7.

Defaults None

Command Modes Policy-map class police configuration mode

Description This command configures the CIR internal queue assignment of a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples Example of setting this parameter.

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# conform-set-tc 3
```

See Also **cbs, conform-set-dscp, conform-set-prec, ebs, eir, exceed-set-dscp, exceed-set-prec, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy, set-priority**

connector

Executes connector mode for the purpose of configuring breakout mode on Quad SFPs (QSFPs).

Synopsis **connector** [**rbridge-id**] *slot/port*
 no connector [**rbridge-id**] *slot/port*

Operands **rbridge-id** Specifies the RBridge ID. This is not valid in standalone mode.
 slot Specifies a valid slot number.
 port Specifies a valid port number.

Defaults None

Command Modes Hardware configuration mode

Descriptions Execute connector mode from hardware configuration mode for the purpose of configuring breakout mode on QSFPs for switches and line cards.

Usage Guidelines None

Examples `switch(config-hardware)# connector 2/0/1`
 `switch(config-connector-2/0/1)#`

See Also **sfp breakout, power-off linecard, power-on linecard, show running-config hardware connector**

continue

Configures a route-map instance number that goes in a **continue** statement in a route-map instance.

Synopsis **continue** *number*
 no continue *number*

Operands *number* Route-map instance number. Range is from 1 through 4294967295.

Defaults None

Command Modes Route map configuration mode

Description Use this command to configure a route-map instance number that goes in a **continue** clause in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

copy

Copies configuration data.

Synopsis `copy source_file destination_file`

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

- default-config** The default configuration.
- global-running-config** Global data of the running configuration. (Available in both fabric cluster mode and logical chassis cluster mode.)
- local-running-configuration** Local data of the running configuration. (Available in fabric cluster mode only.)
- rbridge-running-configuration** *rbridge-id* Running configuration of a specified RBridge. (Available in logical chassis cluster mode only.)
- 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.
- sftp://username:password@host_ip_address/path**
A file on a remote host. Transfer protocol is SFTP.
- usb://path** A file on an attached USB device.

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

- default-config** The default configuration.
- global-running-config** Global data of the running configuration. (Available in both fabric cluster mode and logical chassis cluster mode.)
- local-running-configuration** Local data of the running configuration. (Available in fabric cluster mode only.)
- rbridge-running-configuration** *rbridge-id* Running configuration of a specified RBridge. (Available in logical chassis cluster mode only.)
- 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.
- sftp://username:password@host_ip_address/path**
A file on a remote host. Transfer protocol is SFTP.

2 copy

`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 snapshot (logical chassis cluster mode)

Uploads and downloads configuration snapshot files to and from an FTP or SCP server.

Synopsis **copy snapshot** *rbridge-id rbridge-id snapshot-id snapshot-id* **ftp://directory_path**
copy snapshot *rbridge-id rbridge-id snapshot-id snapshot-id* **scp://directory_path**
copy snapshot **ftp://directory_path** *rbridge-id rbridge-id snapshot-id snapshot-id*
copy snapshot **scp://directory_path** *rbridge-id rbridge-id snapshot-id snapshot-id*

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID whose configuration snapshot has been captured.
snapshot-id *snapshot-id* Specifies the name of the snapshot that has been captured.
directory_path Specifies the FTP or SCP directory path to which you are uploading the snapshot or from which you are downloading the snapshot.

Defaults None

Command Modes Privileged EXEC mode

Description If a snapshot was taken on a node that had been disconnected from the cluster, the cluster will not have the snapshot. Therefore, you can use these commands to upload the snapshot from the disconnected RBridge ID to an ftp or scp server, then download it to an RBridge ID on the cluster.

NOTE

The uploaded snapshot configuration file is stored as a tar file (of the form *rbridgeld-snapshotID*) on the FTP or SCP server.

Usage Guidelines This command applies only to nodes that are members of a logical chassis cluster, not a fabric cluster.

Examples To upload a snapshot configuration file called *node4configuration* to an FTP server:

```
switch# copy snapshot rbridge-id 11 snapshot-id node4configuration  

ftp://backupdir_path
```

See Also **vcs config snapshot (logical chassis cluster mode)**

copy support

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

Synopsis `copy support {ftp | scp | support-param | usb} user user_name password password host ip_address directory dir [sub-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.
	support-param	Enables specification of an optional subdirectory for uploading copy support files.
	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	<i>Specifies a fully qualified path</i> to the directory where the support data will be stored.
	subdirectory dir	<i>Specifies a fully qualified path</i> to the subdirectory where the support data will be stored. (Refer to the Usage Guidelines.)
	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 parameter is not valid in standalone mode and currently not supported.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	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 or 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.OS.txt.ss.gz

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

The subdirectory is appended to the copy support main directory, which is stored as a Distributed Configuration Manager (DCM) configuration item. DCM supports the configuration management of multinode cluster applications and clustering for VCS.

Examples To save support data on an attached USB device:

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

To copy support data to a subdirectory:

```
switch# copy support support-param sub-directory M8 timeout 3
```

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 Use this command to copy 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
- Rbridge ID
- 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
Save to USB device [y/n]: n
Server Name or IP Address: 10.30.33.131
Protocol (ftp, scp): ftp
User: admin
Password: *****
Directory: /home/admin/support
Enter 'all' for all nodes or specify the rbridgeId(s) of the node(s) [Default:
Local Node]: all
Module timeout multiplier[Range:1 to 5.Default:1]: 2
Rbridge-id 195: Saving support information for chassis:sw0, module:RAS...
(output truncated)
```

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

cos-mutation

Specifies the mutation-map to be used on the port.

Synopsis **cos-mutation** *map_name*

Operands *map_name* The user-defined map-name.

Defaults None

Command Modes Policy-map configuration mode

Description Use this command to specify the mutation-map to be used on the port.

Usage Guidelines This command is allowed only for the Ingress direction.

 This command can only be configured in for the **class class-default** command.

 This command can lead to a possible contradiction if there are other user-defined classes used in the same policy-map which has a set CoS action configured. In this case, the defined CoS takes priority over the mutation map.

Examples Typical command example:

```
switch(config)#policy-map mutation  
switch(config-policymap)#class class-default  
switch(config-policyclass)# cos-mutation plsmap
```

See Also **class, policy-map**

cos-traffic-class

Specifies the CoStraffic class mutation map to be used on the port.

Synopsis **cos-traffic-class** *map_name*

Operands *map_name* The user-defined map name.

Defaults None

Command Modes Policy-map configuration mode

Description Use this command to specify the CoStraffic class mutation map to be used on the port.

Usage Guidelines This command is allowed only for the Ingress direction.

This command can only be configured for the **class class-default** command.

This command can lead to a possible contradiction if there are other user-defined classes used in the same policy-map which has a set CoS action configured. In this case, the defined CoS takes priority over the mutation map.

Examples Typical command example:

```
switch(config)#policy-map mutation
switch(config-policymap)#class class-default
switch(config-policyclass)# cos-mutation cos-traffic-class dscp-mutation dscp-cos
dscp-traffic-class plsmap
```

See Also **class**, **policy-map**

counter reliability

Sets and displays the reliability counter for the Access Gateway N_Port Monitoring feature.

Synopsis `counter reliability value`

Operands *value* A value from 10 through 100 static change notifications (SCNs) per 5-minute period.

Defaults 25 SCNs per 5-minute period.

Command Modes Access Gateway (AG) configuration

Description This command is used for the Access Gateway N_Port monitoring feature. The command sets and displays the reliability count of online and offline SCNs counted during a 5-minute period before the link between an N_Port on a VDX switch in Access mode and an F_Port on an FC fabric is considered unreliable.

Usage Guidelines Use this command while in Access Gateway (AG) mode for a specific RBridge ID. Entering the counter reliability command without a value displays the current counter setting. You can set a value from 10 through 100 SCNs per 5-minute period.

Examples Set the reliability counter value.

```
sw0(config-rbridge-id-3-ag)# counter reliability 50
```

Displays the current reliability counter value.

```
sw0(config-rbridge-id-3-ag)# counter reliability
```

See Also None

dampening (BGP)

Sets dampening parameters for the route.

Synopsis **dampening** [*half-life reuse suppress max-suppress-time* | **route-map** *route-map*]
no dampening

Operands	<i>half-life</i>	Number of minutes after which the route penalty becomes half its value. Range is from 1 through 45. Default is 15.
	<i>reuse</i>	Minimum penalty below which the route becomes usable again. Range is from 1 through 20000. Default is 750.
	<i>suppress</i>	Maximum penalty above which the route is suppressed by the device. Range is from 1 through 20000. Default is 2000.
	<i>max-suppress-time</i>	Maximum number of minutes a route can be suppressed by the device.
	route-map	Enables selection of dampening values established in a route map by means of the route-map command.
	<i>route-map</i>	Name of the configured route map.

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to set dampening parameters for a route in BGP address-family mode.

Usage Guidelines Use **dampening** without operands to set default values for all dampening parameters.

To use the dampening values established in a route map, configure the route map first, and then enter **route-map** followed by the name of the configured route map.

A full range of dampening values (*half-life, reuse, suppress, max-suppress-time*) can also be set by means of the **set as-path prepend** command.

Use the **no** form of this command to disable dampening.

Examples To enable default dampening as an address-family function:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# dampening
```

To change the all dampening values as an address-family function:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# dampening 20 200 2500 40
```

To apply the dampening half-life established in a route map, configure the route map and then use the **set dampening** command:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# route-map myroutemap permit 1
switch(config-route-map-myroutemap/permit/1)# set dampening 20
```

See Also route-map, set as-path, set dampening

database-overflow-interval (OSPF)

Configures frequency for monitoring database overflow.

Synopsis **database-overflow-interval** *interval*
no database-overflow-interval

Operands *interval* Time interval at which the device checks to see if the overflow condition has been eliminated. Valid values range from 0 through 86400 seconds.

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

Command Modes OSPF VRF router configuration mode

Description Use this command to specify how long after a router that has entered the OverflowState before it 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 Enter **no database-overflow-interval** to disable the overflow interval configuration.

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

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# router ospf
switch(config-router-ospf-vrf-default-vrf)# database-overflow-interval 60
```

See Also **external-lsdb-limit** (OSPF)

debug access-list-log buffer

Configures ACL buffer characteristics.

Synopsis	debug access-list-log buffer {circular linear} packet count {64-2056} [clear]	
Operands	circular linear	Specifies the buffer type.
	packet count	Specifies a value from 64 through 2056.
	clear	Clears the buffer contents.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to configure buffer characteristics.	
Usage Guidelines	None	
Examples	None	
See Also	None	

debug dhcp packet buffer

Configures a buffer to capture DHCP packets.

Synopsis `debug dhcp packet buffer [circular|linear] [packet-count 64-2056] [vrf vrf-name]`

Operands	circular	Buffer wraps around to overwrite earlier captures.
	linear	Buffer stops capture when the packet-count value is reached.
	packet-count	The maximum number of packets that can be captured in the buffer. Values can be from 64 through 2056. This parameter is necessary when linear is specified.
	64-2056	The range for the maximum number of packets captured in buffer.
	vrf vrf-name	Specifies the Virtual Routing and Forwarding (VRF) instance name mapped to the VRF ID against which you are capturing DHCP packets. If you do not specify vrf vrf-name , the buffer will be captured against the default VRF ID mapped to the <i>vrf-name</i> input.

Defaults The buffer wraps around to overwrite earlier captures (circular).

Command Modes Privileged EXEC mode

Description This command configures the capturing buffer behavior by allowing captures to wrap and overwrite earlier captures or stop capturing when a packet-count limit is reached. The current buffer content is cleared when the configuration changes.

Usage Guidelines None

Examples The following example configures a buffer to capture 510 maximum packets in a circular fashion.

```
sw0# debug dhcp packet buffer circular packet-count 510
```

See Also `show debug dhcp packet buffer`, `debug dhcp packet buffer interface`, `debug dhcp packet buffer clear`

debug dhcp packet buffer clear

Clears buffer content from DHCP packet capture.

Synopsis **debug dhcp packet buffer clear** [**vrf** *vrf-name*]

Operands **vrf** *vrf-name* VRF name mapped to the VRF ID for which the buffer will be cleared. If this operand is not specified, the buffer for the default VRF ID is cleared.

Defaults None

Command Modes Privileged EXEC mode

Description Clears buffer content created from use of the **debug dhcp packet buffer interface** command to enable DHCP packet capture. If the DHCP packet capture is currently enabled, the buffer may fill again.

Usage Guidelines None

Examples The following example clears the buffer content of DHCP packets for a VRF 2.

sw0# debug dhcp packet buffer clear vrf-2

See Also **debug dhcp packet buffer interface**

debug dhcp packet buffer interface

Enables and disables DHCP packet capture on a specific interface.

Synopsis **debug dhcp packet buffer interface** [vlan *vlan_id*] [**gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **fortygigabitethernet** *rbridge-id/slot/port*] [**rx** | **tx**]
no debug dhcp packet buffer interface [vlan *vlan_id*] [**gigabitethernet** *rbridge-id/slot/port* [**rx** | **tx**] | **tengigabitethernet** *rbridge-id/slot/port* | [**rx** | **tx**] **fortygigabitethernet** *rbridge-id/slot/port*] [**rx** | **tx**]
debug dhcp packet buffer all
no debug dhcp packet buffer all

Operands **all** Enables DHCP packet capture on all switch interfaces.

vlan *vlan_id* VLAN identification of the interface where you want to enable or disable DHCP packet buffer capture.

gigabitethernet *rbridge-id/slot/port* A valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

rx | **tx** Specifies whether to capture transmitted or received packets. If not specified, both are captured.

tengigabitethernet *rbridge-id/slot/port* A valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

rx | **tx** Specifies whether to capture transmitted or received packets. If not specified, both are captured.

fortygigabitethernet *rbridge-id/slot/port* A valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

rx | **tx** Specifies whether to capture transmitted or received packets. If not specified, both are captured.

Defaults None

Command Modes Privileged EXEC mode

Description Enables or disables capture of DHCP packets on all or specified interfaces.

Usage Guidelines The **all** operand replaces the *interface* operand.

Use the **no** form of this command to disable DHCP packet capture on a specific switch interface when used with **debug dhcp packet buffer interface** [*interface specifications*]

2 debug dhcp packet buffer interface

Use the **no** form of this command to disable the DHCP packet capture on all switch interfaces when used with **debug dhcp packet buffer all**.

You can specify a VLAN or physical port for capturing packets. If an interface is not specified, packets are captured on all interfaces.

On the Brocade VDX family of switches, VLANs are treated as interfaces for configuration purposes. By default, all DCB ports are assigned to VLAN 1 (VLAN ID equals 1). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086. (VLAN IDs 4087 through 4095 are reserved on these switches.)
- On all other Brocade VDX switches: 1 through 3962. (VLAN IDs 3963 through 4095 are reserved on these switches.)

The **gigabitethernet rbridge-id/slot/port** parameter is used only on the Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches. The prompt for configuring these ports is in the following format:

```
sw0(config-if-gi-22/0/1)#
```

Examples

The following command enables DHCP packet capture for transmitting data on forty-gigabit Ethernet interface 1/0/1.

```
sw0# Debug dhcp packet buffer interface te 1/0/1 tx
```

The following command enables DHCP packet capture for receiving data on forty-gigabit Ethernet interface 1/0/1.

```
sw0# No debug dhcp packet buffer interface te 1/0/1 rx
```

The following command enables DHCP packet capture on all switch interfaces of switch 0.

```
sw0# debug dhcp packet buffer all
```

The following command disables DHCP packet capture on all switch interfaces of switch 0.

```
sw0# no debug dhcp packet buffer all
```

See Also

debug dhcp packet buffer clear, debug dhcp packet buffer, show debug dhcp packet, debug fcoe show swcfg

debug fcoe show swcfg

Displays information related to FCoE classified VLAN configuration in a Virtual Fabrics context, as well as other parameters.

Synopsis **debug fcoe show swcfg**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view information related to FCoE classified VLAN configuration in a Virtual Fabrics context, as well as other parameters.

Usage Guidelines None

Examples The following example shows typical output of this command.

```
switch# debug fcoe show swcfg
sw#  vlan  ivid      ctag      Dom  fcmap      Pri  Intvl  Tout
=====
0    1002  0x3ea      0x0      10   0x0efc00  3    8000   0
0    0      0x0      0x0      10   0x000000  0     0     0
0    0      0x0      0x0      10   0x000000  0     0     0
0    0      0x0      0x0      10   0x000000  0     0     0
0    0      0x0      0x0      10   0x000000  0     0     0
0    0      0x0      0x0      10   0x000000  0     0     0
0    0      0x0      0x0      10   0x000000  0     0     0
0    0      0x0      0x0      10   0x000000  0     0     0
```

See Also None

debug ip

Enables debugging for the IGMP and ICMP traffic on the switch.

Synopsis **debug ip packet** [**interface** *interface-type interface-number* [**vlan** *vlan_id*] | **count** {**tx** | **rx**} | **icmp** [**interface** *interface-type interface-number*] | **count** *value* | **tx** | **rx** | **igmp** [**interface** *interface-type interface-number*] | **all** | **group** *mcast-grp-address*]

no debug ip packet

Operands	packet	Enables IP packet debugging.
	interface	Displays the IP traffic for the specified interface only.
	<i>interface-type</i>	Network interface type (external 10-gigabit Ethernet interface, port-channel, or VLAN).
	<i>interface-number</i>	Layer 2 or Layer 3 interface number.
	vlan <i>vlan_id</i>	Specifies a VLAN. (Refer to the Usage Guidelines.)
	count <i>value</i>	Stops display after display count packets. Valid values range 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.
	<i>mcast-grp-address</i>	Multicast group address.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to enable or disable debugging for IP. This will display all IGMP or ICMP packets received or transmitted. This can be enabled globally, per interface, or on a multicast group.

Usage Guidelines Use the **no** form of this command to disable debugging.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also None

debug ip bgp

Displays information related to the processing of BGP4, with a variety of options.

Synopsis **debug ip bgp** [**cli** | **dampening** | | **events** | **general** | **ip-prefix** *ip-addr/mask-len* | **ip-prefix-list** *name* **keepalives** | **neighbor** | **route-map** *route-selection* | | **traces** | **updates** [**rx** | **tx**]]

no debug ip bgp

Operands	address-family	Displays information about address-family mode.
	cli	Displays information about BGP CLI
	dampening	Displays BGP4 dampening.
	events	Displays all BGP4 events.
	general	Displays BGP4 common events.
	graceful-restart	Displays BGP graceful restart events.
	ip-prefix	Displays information filtered by IP prefix.
	<i>ip-addr</i>	IPv4 address in dotted-decimal notation.
	<i>mask-len</i>	IPv4 mask length in CIDR notation.
	ip-prefix-list	Displays information filtered by IP prefix list.
	<i>name</i>	Name of IP prefix list.
	keepalives	Displays BGP4 keepalives.
	neighbor	Displays BGP information for specified neighbor router.
	packet	Displays information about BGP packets.
	route-map	Displays configured route map tags.
	route-selection	Displays BGP4 route selection.
	traces	Displays BGP traces.
	updates	Displays BGP4 updates.
	rx	Displays BGP4 received updates.
	tx	Displays BGP4 transmitted updates

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view information related to the processing of BGP4, with a variety of options.

Usage Guidelines Use the **no** form of this command to disable debugging.

Examples To view all BGP4 events:

```
switch# debug ip bgp events
```

See Also None

debug ip bgp address-family ipv4 unicast

Displays information related to the processing of IPv4 address-family support in BGP4.

Synopsis **debug ip bgp address-family ipv4 unicast**
no debug ip bgp address-family ipv4 unicast

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view information related to the processing of IPv4 address-family support in BGP4.

Usage Guidelines Use the **no** form of this command to disable debugging.

Examples Example of typical command.

switch# **debug ip bgp address-family ipv4 unicast**

See Also None

debug ip bgp neighbor

Displays information related to the processing of BGP4 for a specific neighbor.

Synopsis **debug ip bgp neighbor** *ip-addr*
 no debug ip bgp neighbor *ip-addr*

Operands *ip-addr* IPv4 address in dotted-decimal notation.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view information related to the processing of BGP4 for a specific neighbor.

Usage Guidelines Use the **no** form of this command to disable debugging.

Examples Typical command structure.
 switch# **debug ip bgp neighbor 10.11.12.13**

See Also None

debug ip igmp

Enables debugging for 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*}}

no debug ip igmp

Operands	all	Displays all values.
	group <i>A.B.C.D</i>	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 parameter to specify the interface to be monitored.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
	vlan <i>vlan_id</i>	Specifies which VLAN interface to display the snooping configuration related information. Refer to the Usage Guidelines.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to enable or disable debugging for IGMP. This will display all of the IGMP packets received and sent, and IGMP-host related events.

Usage Guidelines Use the **no** form of this command to disable debugging.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

2 debug ip igmp

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also None

debug ip ospf

Enables debugging for the IP Open Shortest Path First (OSPF) protocol.

Synopsis **debug ip ospf** {**adj** | **all-vrfs** | **dev** | **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** | **vrf** *name*}

no debug ip ospf

Operands	adj	Adjacency related debugs.
	all-vrfs	Information for all VRFs instances in a cluster.
	dev	Developer debug options.
	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 <i>A.B.C.D</i>	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 <i>A.B.C.D</i>	Neighbor debugging for the neighbor that you specify.
	packet	Packet debugs.
	retransmission	Retransmission events.
	route <i>A.B.C.D</i>	Route debugs for the router that you specify.
	spf	SPF trace.
	vrf <i>name</i>	Debug information for VRF.

Defaults IP OPSF debugging is disabled.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable debugging for IP OPSF traffic.

Usage Guidelines Enter **no debug ip ospf** to disable IP OPSF debugging.

Examples To enable adjacency-related debugs:

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

See Also None

debug ip pim

Enables debugging for IP Protocol Independent Multicast.

Synopsis **debug ip pim** {**add-del-oif** | **bootstrap** | **group** | **join-prune** | **nbr-change** | **packets** | **parent** | **regproc** | **route-change** | **rp** | **source** | **state** | **all**}

no debug ip pim all

Operands	add-del-oif	Controls the OIF change flag.
	bootstrap	Controls the bootstrap processing flag.
	group	Controls the processing for a group flag.
	join-prune	Controls the Join/Prune processing flag.
	nbr-change	Controls the neighbor changes flag.
	packets	Controls the packet processing flag.
	parent	Controls the parent change processing flag.
	regproc	Controls the register processing flag.
	route-change	Controls the route changes flag.
	rp	Controls the Rendezvous Point (RP) processing flag.
	source	Controls the processing for a source flag.
	state	Controls the state processing flag.
	all	Controls all of the states.

Defaults All flags are disabled.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable debugging for IP Protocol Independent Multicast.

Usage Guidelines Use the **no debug ip pim all** command to disable debugging.

Examples None

See Also None

debug ip rtm

Enables debugging for IP RTM.

Synopsis `debug ip rtm {A.B.C.D | all | counters {clear | show} dump | errors | fib-comm | nexthop | port | vrf}`

Operands

<code>A.B.C.D</code>	Debugs the route specified by this IP address.
<code>all</code>	Enables all debugs.
<code>counters</code>	Enables debug counters.
<code>clear</code>	Clears debug counters.
<code>show</code>	Shows debug counters.
<code>dump</code>	Shows database dump.
<code>errors</code>	Enables internal error debugs.
<code>fib-comm</code>	Debugs communications between the forwarding information base and the routing table manager.
<code>nexthop</code>	Enables next-hop debugs.
<code>port</code>	Enables port database debugs.
<code>vrf</code>	Enables VRF debugs.

Defaults IP RTM debugging is disabled.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable debugging for IP route management.

Usage Guidelines None

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

```
switch# debug ip rtm 192.145.12.1
```

To show a database dump:

```
switch# 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
```

2 debug ip rtm

```
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
```

See Also None

debug ip vrf

Displays information related to VRF.

Synopsis **debug ip vrf** *ip-addr*
no debug ip vrf

Operands *ip-addr* IPv4 address in dotted-decimal notation.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view information related to VRF.

Usage Guidelines Use the **no** form of this command to disable debugging.

Examples Typical command structure.

```
switch# debug ip vrf
```

See Also None

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 **fortygigabitethernet** *rbridge-id/slot/port* | 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 <i>rbridge-id/slot/port</i>	Specifies the 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the routing bridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	interface gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the routing bridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies the 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the routing bridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	interface tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies the 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the routing bridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.

port Specifies a valid port number.

interface gigabitethernet *rbridge-id/slot/port*
Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the routing bridge ID. 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. Valid values range from 1 through 7.

Defaults LACP debugging is disabled.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable debugging for Link Aggregation Control Protocol (LACP).

Usage Guidelines Enter **terminal monitor** to display debugging outputs on a particular cmsh session.
Enter **no debug lacp** to disable LACP debugging.

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 dump

Dumps the LLDP debug information to the console.

Synopsis `debug lldp dump {all | [interface tengigabitethernet rbridge-id/slot/port | gigabitethernet rbridge-id/slot/port] [both]] | [detail [both | rx | tx]]`
`no debug lldp dump {all | interface tengigabitethernet slot/port}`

Operands	all	Dumps all information to the console.
	interface	Use this parameter to specify the interface to be monitored.
	tengigabitethernet	<i>rbridge-id/slot/port</i> Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the routing bridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet	<i>rbridge-id/slot/port</i> Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the routing bridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 LLDP debugging is disabled.

Command Modes Privileged EXEC mode

Description	Use this command to dump debugging information for Link Layer Discovery Protocol (LLDP) to the console.

Usage Guidelines	None

Examples Typical use of this command.

```
switch# debug lldp dump all
LLDP Interface Debug Information for Te 1/0/3
Admin Status:  RX_TX
Associated Profile:
Link-level FCoE Priority: 0x08 (Configured: No)
Link-level iSCSI Priority: 0x10 (Configured: No)
Link Properties:
    CEE Incapable
    FCoE LLS not Ready
    FCF-Forward Disabled
```

```
Sending TLVs:
  CHASSIS_ID: 0x00051ecd226a (MAC)
  PORT_ID: Te 1/0/3 (IF Name)
  TTL: Hold (4) x Interval (30)
  IEEE_DCBX
  DCBX_FCOE_APP
  DCBX_FCOE_LOGICAL_LINK
  Configured FCoE App
  Configured FCoE Link
  DCBX_CTRL
<truncated>
```

See Also **show debug lldp**

debug lldp packet

Enables debugging for the Link Layer Discovery Protocol (LLDP).

Synopsis `debug lldp packet {all | [interface fortygigabitethernet rbridge-id/slot/port | tengigabitethernet rbridge-id/slot/port | gigabitethernet rbridge-id/slot/port] [both]] | [detail [both | rx | tx]]`

`no debug lldp packet {all | interface fortygigabitethernet rbridge-id/slot/port | tengigabitethernet slot/port | gigabitethernet rbridge-id/slot/port}`

Operands	all	Turns on LLDP packet debugging on all interfaces.
	interface	Use this parameter to specify the interface to be monitored.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 LLDP debugging is disabled.

Command Modes Privileged EXEC mode

Description	Use this command to enable or disable debugging for Link Layer Discovery Protocol (LLDP).

Usage Guidelines	Enter terminal monitor to display debugging outputs on a particular cmsh session. Enter no debug lldp packet to disable LLDP debugging.

Examples To enable debugging of LLDP for both received and transmitted packets on the 10-gigabit 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 lldp dump

Dumps the Link Layer Discovery Protocol (LLDP) data to the console.

Synopsis **debug lldp dump** {**all** | [**interface fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]}

Operands **all** Turns on LLDP packet debugging on all interfaces.

interface Use this parameter to specify the interface to be monitored.

fortygigabitethernet *rbridge-id/slot/port*
 Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This 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-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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 dump Link Layer Discovery Protocol (LLDP) to the console.

Usage Guidelines None

Examples None

See Also **show debug lldp**

debug spanning-tree

Enables debugging for the Spanning Tree Protocol (STP).

Synopsis `debug spanning-tree {all | bpdu [rx | tx [all | interface port-channel number | fortygigabitethernet slot/port | tengigabitethernet slot/port | gigabitethernet slot/port]]`
`no debug spanning-tree {all | bpdu [rx | tx [all | interface port-channel number | fortygigabitethernet slot/port | 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 parameter to specify the interface to be monitored.
port-channel <i>number</i>	Specifies the port-channel interface. Valid values range from 1 through 6144.
fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.

Defaults STP debugging is disabled.

Command Modes Privileged EXEC mode

Description Use this command to enable or disable debugging for STP.

Usage Guidelines Enter **terminal monitor** to display debugging outputs.
 Enter **no debug spanning-tree** to disable debugging.

Examples To enable debugging of spanning-tree for both Rx and Tx on the 10-gigabit 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
```

2 debug spanning-tree

```
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 udd
```

Enables debugging for the UniDirectional Link Detection (UDLD) protocol.

Synopsis `debug uddl packet [all | {interface [fortygigabitethernet rbridge-id/slot/port | gigabitethernet rbridge-id/slot/port | tengigabitethernet rbridge-id/slot/port]} {both | rx | tx}`

no debug udid packet

Operands	all	Activates UDLD debugging on all ports on the switch.

fortygigabitethernet *rbridge-id/slot/port*

Specifies a valid 40-gigabit Ethernet interface for setting debugging.

<i>rbridge-id</i>	Specifies the RBridge ID.

<i>slot</i>	Specifies a valid slot number.

<i>port</i>	Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*

Specifies a valid 1-gigabit Ethernet interface for setting debugging.

<i>rbridge-id</i>	Specifies the RBridge ID.

<i>slot</i>	Specifies a valid slot number.

<i>port</i>	Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*

Specifies a valid 10-gigabit Ethernet interface for setting debugging.

<i>rbridge-id</i>	Specifies the RBridge ID.

<i>slot</i>	Specifies a valid slot number.

port Specifies a valid port number.

both Sets debugging for both received and transmitted packets.

rx	Sets debugging for received packets only.

tx	Sets debugging for transmitted packets only.

Defaults UDLD debugging is disabled.

Command Modes Privileged EXEC mode

Description	Use this command to turn on dumping of UDLD PDUs as they are transmitted and/or received on one or all ports. You can use the show debug udld command to view your current debug settings.

Usage Guidelines	Use the no form of this command to turn off either all dumping of UDLD PDUs or dumping on a specific port.

Examples To turn on debugging of transmitted packets on a specific tengigabitethernet interface:

```
switch# debug uddl packet interface te 5/0/1 tx
```

See Also `show debug udd`

debug vrrp

Enables debugging for the Virtual Router Redundancy Protocol (VRRP).

Synopsis	debug vrrp all	
	debug vrrp events	
	debug vrrp packets { interface { port-channel <i>number</i> fortygigabitethernet <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i> tengigabitethernet <i>rbridge-id/slot/port</i> } ve <i>vlan_id</i> [recv sent]}	
	debug vrrp session <i>VRID</i>	
	no debug vrrp all	
	no debug vrrp events	
	no debug vrrp packets { interface { port-channel <i>number</i> fortygigabitethernet <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i> tengigabitethernet <i>rbridge-id/slot/port</i> } recv sent }	
	no debug vrrp session <i>VRID</i>	
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 <i>recv</i> and <i>sent</i> parameters.
	port-channel <i>number</i>	Specifies the port-channel interface. Valid values range from 1 through 63.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet port interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This parameter is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.

<i>port</i>	Specifies a valid port number.
ve <i>vlan_id</i>	Specifies the VLAN number for a virtual Ethernet (VE) interface.
packets recv	Debugs packets received.
packets sent	Debugs packets sent.
session <i>VRID</i>	Specifies the virtual group ID to debug. Valid values range from 1 through 128.

Defaults	None
Command Modes	Privileged EXEC mode
Description	Use this command to enable or disable debugging for VRRP traffic. 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. Enter no debug vrrp all with to disable all VRRP debugging. Enter no debug vrrp followed by specific events or packet parameters to remove a specific VRRP debugging configuration.
Examples	To set debugging on sent and received packets for a 10-gigabit Ethernet interface that has an <i>rbridge-id/slot/port</i> of 121/0/50: <pre>switch# debug vrrp packets interface tengigabitethernet 121/0/50</pre> To set debugging for a session for a VRRP virtual group called <i>vrrp-group-25</i>: <pre>switch# debug vrrp session 25</pre>
See Also	vrrp-extended-group, vrrp-group

default-information-originate (BGP)

Configures the device to originate and advertise a default route.

Synopsis **default-information-originate**
 no default-information-originate

Operands None

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to configure the device to originate and advertise a default BGP4 route.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To originate and advertise a default BGP4 route:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# address-family ipv4 unicast  
switch(config-bgp-ipv4u)# default-information-originate
```

See Also None

default-information-originate (OSPF)

Controls distribution of default information.

Synopsis **default-information-originate** [**always**] [**metric** *metric*] [**metric-type** {**type-1** | **type-2**}]
no default-information-originate

Operands

always	Always 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 <i>metric</i>	Used for generating the default route, this parameter specifies the cost for reaching the rest of the world through this route. If you omit this parameter and do not specify a value using the <i>default-metric</i> router configuration command, a default metric value of 1 is used. Valid values range from 1 through 65535. The default is 10.
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.

Defaults The default values vary depending on the Operands settings.

Command Modes OSPF VRF router configuration mode

Description Use this command to control distribution of default information to OSPF router. This provides criteria for the redistribution of any default routes found in the route table manager (whether static or learned from another protocol) to its neighbors.

Usage Guidelines Enter **no default-information-originate** to disable this command.

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

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# default-information-originate always
metric 20
```

See Also **default-metric (OSPF), metric-type (OSPF)**

default-local-preference (BGP)

Enables setting of a local preference value to indicate a degree of preference for a route relative to that of other routes.

Synopsis **default-local-preference** *num*
 no default-local-preference

Operands *num* Local preference value. Range is from 0 through 65535.

Defaults The default local preference is 100.

Command Modes BGP configuration mode

Description Local preference indicates a degree of preference for a route relative to that of other routes. BGP4 neighbors can send the local preference value as an attribute of a route in an UPDATE message. Use this command to change the local preference value.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples `switch(config)# rbridge-id 10`
 `switch(config-rbridge-id-10)# router bgp`
 `switch(config-bgp-router)# default-local-preference 200`

See Also None

default-metric (BGP)

Changes the default metric used for redistribution.

Synopsis **default-metric** *value*
 no default-metric

Operands *value* Metric value. Range is from 0 through 65535.

Defaults The default metric value is 0.

Command Modes BGP address-family IPv4 unicast configuration mode

Description When routes are selected, lower metric values are preferred over higher ones. The default, the BGP4 Multi-Exit Discriminator (MED) value, is not assigned. Use this command to change the metric value.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To configure the device to compare MEDs:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# address-family ipv4 unicast  
switch(config-bgp-ipv4u)# default-metric 100
```

See Also None

default-metric (OSPF)

Sets the default metric value for the OSPF routing protocol.

Synopsis **default-metric** *metric*
 no default-metric

Operands *metric* OSPF routing protocol metric value.

Defaults The default metric value for the OSPF routing protocol is 10.

Command Modes OSPF VRF router configuration mode

Description Use this command to specify a default metric which will overwrite 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 Enter **no default-metric** to return to the default setting.

Examples To set the default metric to 20:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# default-metric 20
```

See Also **default-information-originate (OSPF)**

default-passive-interface (OSPF)

Marks all OSPF interfaces passive by default.

Synopsis **default-passive-interface**
 no default-passive-interface

Operands None

Defaults None

Command Modes OSPF VRF router configuration mode

Description Use this command if you want all OSPF interfaces marked passive by default.

You can use the **ip ospf active** and **ip ospf passive** commands in interface subconfiguration mode to change active/passive state on specific OSPF interfaces.

Usage Guidelines Use the **no** form of this command to disable it.

Examples To mark all OSP interfaces as passive for a specified RBridge:

```
switch# configure  
switch(config)# rbridge-id 1  
switch(config-rbridge-id-1)# router ospf  
switch(config-router-ospf-vrf-default-vrf)# default-passive-interface
```

See Also None

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/mask*} [**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS/mask*] [*EtherType* | **arp** | **fcoe** | **ipv4**] [**count**] [**log**]

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

Operands

any	Specifies any source MAC address.
host <i>MAC_ADDRESS</i>	Specifies the source host MAC address for which to set deny conditions. Use the format HHHH.HHHH.HHHH.
<i>MAC_ADDRESS</i>	Specifies the destination host MAC address for which to set deny conditions. Use the format HHHH.HHHH.HHHH.
<i>mask</i>	Specifies the mask for the associated host MAC address.
any	Specifies any destination MAC address.
host <i>MAC_ADDRESS</i>	Specifies the source host address for which to set deny conditions. Use the format HHHH.HHHH.HHHH.
<i>MAC_ADDRESS</i>	Specifies the destination host address for which to set deny conditions. Use the format HHHH.HHHH.HHHH.
<i>EtherType</i>	Specifies the protocol number for which to set the deny conditions. Valid values range 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.
log	Enables the logging feature.

Defaults No MAC addresses are subjected to traffic dropping.

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. The counters supported per port group vary based on platform.

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.

2 deny (extended ACLs)

- The order of the rules in an ACL is critical. The first rule that matches the traffic stops further processing of the frames. Rules containing specific information should be listed first, followed by rules that contain more general information.
- Enter **no deny any** to deny any rule that was added earlier.
- Enter **no deny** followed by specific address parameters to remove traffic dropping for a specific MAC address configuration.

Examples To create a rule in a MAC extended address to drop IPv4 traffic from the source MAC address 0022.3333.4444/255.255.0.0 to the destination MAC address 0022.3333.5555/255.255.0.0 and to enable the counting of packets:

```
switch(config-macl-ext)# deny 0022.3333.4444 0022.3333.5555 255.255.0.0 ipv4 count
```

To delete a rule from a MAC extended address:

```
switch(config-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*/*mask* | **any**} [**count**]
 no deny {*MAC_ADDRESS*/*mask* | **any**}

Operands *MAC_ADDRESS* Specifies the source host MAC address for which to set deny conditions. The correct format is: HHHH.HHHH.HHHH.
 mask Specifies the mask for the associated host MAC address.
 any Specifies any source MAC address.
 count Enables counting of the packets matching the rule.

Defaults No MAC ACLs are subjected to traffic dropping.

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. 255 ACL counters are supported per port group.

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.

- The order of the rules in an ACL is critical. The first rule that matches the traffic stops further processing of the frames. Rules containing specific information should be listed first, followed by rules that contain more general information.
- Enter **no deny any** to deny any rule that was added earlier.
- Enter **no deny any** to deny any rule that was added earlier.
- Enter **no deny** followed by a specific address to remove traffic dropping for a from the specified MAC address.

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 0022.3333.4444/255.255.0.0 count
```

To delete a rule from a MAC standard ACL:

```
switch(conf-macl-std)# no deny 0022.3333.4444/255.255.0.0
```

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 string must be between 1 and 63 ASCII characters in length.

Defaults None

Command Modes Interface subtype configuration mode

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

Usage Guidelines Enter **no description** to remove the interface description.

Examples To set the string describing internal 10-gigabit Ethernet 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 LLDP description.

Synopsis **description** *line*
 no description

Operands *line* Characters describing LLDP. The string must be between 1 and 50 ASCII characters in length.

Defaults None

Command Modes Protocol LLDP configuration mode

Description Use this command to specify the description of the LLDP.

Usage Guidelines Enter **no description** to remove the LLDP description.

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 string that contains the description of the Port Mirroring session. The string must be between 1 and 64 ASCII characters in length.

Defaults None

Command Modes Monitor session configuration mode

Description Use this command to specify a label displayed in the running-config file to describe the Port Mirroring session.

Usage Guidelines Enter **no description** to remove the port mirroring description.

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**

description (VRRP)

Describes a VRRP-E interface.

Synopsis **description** *description*
 no description

Operands *description* Characters describing the VRRP-E interface. The string must be between 1 and 64 ASCII characters in length.

Defaults None

Command Modes Virtual-router-group configuration mode

Description Use this command to describe a VRRP-E interface.

Usage Guidelines Enter **no description** to remove the description.

Examples To describe VRRP-E group 10 interface:

```
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)# description vrrpe_group_10
```

See Also **vrrp-group, vrrp-extended-group**

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*
 no desire-distance

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

Defaults The default is 0.

Command Modes Interface Fibre Channel configuration mode

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.

Use the no form of this command to disable it.

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 1s
switch(config-FibreChannel-7/0/2)# desire-distance 100
```

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

dhcp auto-deployment enable

Enables DHCP auto-deployment on the switch.

Synopsis **dhcp auto-deployment enable**

Operands None

Defaults Disabled

Command Modes Privileged EXEC mode

Description Use this command to enable DHCP auto-deployment on the switch.

Usage Guidelines This command will cause a cold/disruptive reboot and will require that Telnet, secure Telnet, or SSH sessions be restarted.

Scenario 1: When you enable DHCP auto-deployment and the system starts to reboot, the DAD process is triggered after configuration replay is complete.

In the case of dual Management Moddule (MM) chassis, the DAD process waits for the dual MMs to be in sync before starting the requested firmware download. However, if you manually issue **firmwaredownload -sb** during this period (after DAD is triggered and before the MM is in sync), DHCP auto-deployment will fail because the previous firmware download takes precedence. If you manually issue **firmwaredownload -sb** before DAD is triggered, DHCP auto-deployment will fail for the same reason.

Scenario 2: You issue the command to enable DAD (answer “Yes” when prompted), but before the system reboot, there is an HA failover. DAD will be cancelled. You must enable DHCP auto-deployment from the new active switch.

Scenario 3: You issue the command to enable DAD, but after the system reboot is invoked, takeover occurs (the previous standby switch becomes the new active switch), DHCP auto-deployment will proceed.

Scenario 4: You manually issue the **firmwaredownload** command, but before the firmware download is completed, you enable DAD from the CLI and answer “Yes” when prompted to reboot the switch. When the switch boots up, even if the DAD process detects that the firmware download is needed, it will fail during the sanity check because the previous incomplete firmware download takes precedence. DHCP auto-deployment will fail.

Examples None

See Also **show dadstatus**

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 Typical output for this command.

```
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.

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

Operands	action <i>pattern</i>	Specifies the LED pattern. Action choices are as follows:
	<i>blink-amber</i>	Blink Port status LED amber
	<i>blink-green</i>	Blink Port status LED green
	<i>cycle-all</i>	Cycle all Port LEDs
	<i>status-amber</i>	Turn Port status LED amber
	<i>status-green</i>	Turn Port status LED green
	<i>turn-off</i>	Turn Port status LED off
	ethernet	The logical Ethernet interface name, which is mutually exclusive from the Fibre Channel parameter. By default, all ports are tested.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number
	fibrechannel	The logical Fibre Channel interface name, which is mutually exclusive from the Ethernet parameter. By default, all ports are tested.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	npass <i>count</i>	Specifies the number of times to perform this test. Valid values range from 1 through 10. The default value is 1.
	slot <i>slot_id</i>	Specifies the slot identifiers for slot-based systems only.

Defaults 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).

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.



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.

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.

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 parameter. By default, all ports are tested.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number
	fibrechannel	The logical Fibre Channel interface name, which is mutually exclusive from the Ethernet parameter. By default, all ports are tested.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	lbmode <i>mode</i>	Specifies the loopback point for the test. Valid values are 1 (external) or 2 (internal). The default is 2.
	nframes <i>count</i>	Specifies the number of frames to send. Valid values range from 1 through 16. The default is 16.
	slot <i>slot_id</i>	Specifies the slot identifiers for slot-based systems only.
	spdmode <i>mode</i>	Specifies the speed mode for the test. This parameter controls the speed at which each port operates during the test. Valid parameters are as follows: 1 Gbps 2 Gbps 4 Gbps 8 Gbps 10 Gbps 16 Gbps 40 Gbps 100 Gbps

Defaults Number of frames (**nframes**) is 16.

Loopback mode (**lbmode**) is 2.

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** 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 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.

**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.

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 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.

Enter **no diag post** [*rbridge-id*] **enable** to disable the POST for that RBridge.

Examples To enable the POST for a RBridge:

```
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 the POST for a RBridge:

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

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

diag prbtest

Runs the Pseudo Random Bit Sequence (PRBS) test on a given slot to verify the back end 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.

Synopsis `diag prbtest slot {L1 | L2 | S1 | S2 ...} pattern {pattern}`

Operands

slot <i>slot</i>	Specifies the slot ID, from 1 through 6. This test is applicable for slot-based systems only.
pattern <i>pattern</i>	Specifies the PRBS pattern, from 1 through 8. 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 back end connections between LC and SFM. This command also verifies the internal blade connections when executed in LC.

Usage Guidelines 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.



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.

Examples In slot-based switches:

```
switch# diag prbtest slot L6 pattern PRBS7
% Info: This test should be run to completion. Please do not abort while it is
executing.
Running prbtest...
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
<..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
```

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	Referto the Usage Guidelines.
Command Modes	Privileged EXEC mode
Description	Use this command to set the user-defined parameters for running a system verification test.
Usage Guidelines	If, after you enter the diag setcycle command, you respond with yes, the following settings are the default values: • <i>num_of_runs</i>: 1. Valid values for number of runs are 1 through 25. • <i>min_lb_mode</i>: 2. Valid values for minimum loopback mode are 1 (external) or 2 (internal). If set to 1, all the external user ports must be connected with small form-factor pluggable devices (SFPs) and loopback plugs. • <i>pled_passes</i>: 1. Valid values for the number of portLedTest loops are 1 through 10. • <i>tbr_passes</i>: 1. Valid values for the number of turboRamTest loops are 1 through 10. This parameter is not supported on fixed configuration switches. • <i>plb_nframes</i>: 16. Valid values for the number of portLoopbackTests are 4 through 16. If you respond with no, the system prompts you for these values.

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.
ronteel28# 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.

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 <i>short</i> 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.	



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 parameter, 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.

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.

Synopsis	diag turboramtest [passcnt <i>count</i>] [slot <i>slot_id</i>]	
Operands	passcnt <i>count</i>	Specifies the number of test repetitions. By default, the test runs once. Valid values range from 1 through 10.
	slot <i>slot_id</i>	Specifies the slot ID. This is mandatory for slot-based systems only.
Defaults	The pass count (passcnt) is 1.	
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	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.	



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.

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.
```

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 (BGP)

Changes the default administrative distances for EBGp, IBGP, and local BGP4.

Synopsis **distance** *external-distance internal-distance local-distance*
no distance

Operands *external-distance* EBGp distance. Range is from 1 through 255.
 internal-distance IBGP distance. Range is from 1 through 255.
 local-distance Local BGP4 distance. Range is from 1 through 255.

Defaults None

Command Modes BGP configuration mode

Description To select one route over another according to the source of the route information, the device can use the administrative distances assigned to the sources. The administrative distance is a protocol-independent metric that IP devices use to compare routes from different sources. Lower administrative distances are preferred over higher ones. Use this command to change the default administrative distances for EBGp, IBGP, and local BGP4.

Usage Guidelines Enter values in the order corresponding to the values in Operands.
 Use the **no** form of this command to restore the defaults.

Examples To configure the device to change the administrative distance:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# distance 100 150 200
```

See Also None

distance (OSPF)

Configures an administrative distance value for OSPF routes.

Synopsis **distance** {**external** | **inter-area** | **intra-area**} *distance*
no 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. Valid values range from 1 through 255. The default is 110.

Defaults The administrative distance value for OSPF routes is 110.

Command Modes OSPF VRF router configuration mode

Description Use this command to specify 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 Enter **no distance** to return to the default setting.

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

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# distance external 125
```

See Also None

distribute-list route-map (OSPF)

Creates a route-map distribution list.

Synopsis **distribute-list route-map** *map* **in**
 no distribute-list route-map

Operands *map* Name of a route map.
 in Creates a distribution list for an inbound route map.

Defaults None

Command Modes OSPF VRF router configuration mode

Description Use this command to create a distribution list that can filter Link State Advertisements (LSAs) received from other OSPF routers before adding the corresponding routes to the routing table.

Usage Guidelines Enter **no distribute-list route-map** to remove the distribution list.

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

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# distribute-list route-map filter1 in
```

See Also None

dot1x authentication

Enables 802.1X authentication on a port.

Synopsis **dot1x authentication**
 no dot1x authentication

Operands None

Defaults 802.1X authentication is disabled for ports.

Command Modes Interface subtype configuration mode

Description Use this command to enable 802.1X authentication on a specific port.

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

Examples To enable 802.1X authentication on a specific 10-gigabit Ethernet interface port:

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

To disable 802.1X authentication on a specific 40-gigabit Ethernet 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 Authentication is disabled globally.

Command Modes Global configuration mode

Description Use this command to globally enable 802.1X authentication.

Usage Guidelines Enter **no dot1x enable** to disable 802.1X authentication globally.

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.

force-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 subtype configuration mode

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

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

Examples To enable the port state to auto on a specific 10-gigabit Ethernet 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 40 -gigabit Ethernet 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 between attempts at authentication. Valid values range from 1 through 65535 seconds.

Defaults 60 seconds

Command Modes Interface subtype configuration mode

Description Use this command to set the time in seconds a switch waits before attempting to perform authentication after a failed authentication. When a switch cannot authenticate a client, the switch remains idle for the 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.

Enter **no dot1x quiet-period** to return to the default setting.

Examples To change the interval time to 200 seconds on a specific 10-gigabit Ethernet 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 40-gigabit Ethernet 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 802.1X reauthentication on a specified interface.

Synopsis	dot1x reauthenticate interface [tengigabitethernet <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i>]
Operands	tengigabitethernet <i>rbridge-id/slot/port</i> Specifies a valid 10-gigabit Ethernet interface. <i>rbridge-id</i> Specifies the RBridge ID. This is not valid in standalone mode. <i>slot</i> Specifies a valid slot number. <i>port</i> Specifies a valid port number. gigabitethernet <i>rbridge-id/slot/port</i> Specifies a valid 1-gigabit Ethernet interface. <i>rbridge-id</i> Specifies the RBridge ID. This is not valid in standalone mode. <i>slot</i> Specifies a valid slot number. <i>port</i> Specifies a valid port number.
Defaults	None
Command Modes	Privileged EXEC mode
Description	Use this command to initiate 802.1X reauthentication on a specified interface.
Usage Guidelines	None
Examples	To initiate reauthentication on 10-gigabit Ethernet interface 0/16: <pre>switch# dot1x reauthenticate interface tengigabitethernet 0/16</pre>
See Also	None

dot1x reauthentication

Enables 802.1X port reauthentication.

Synopsis **dot1x reauthentication**
 no dot1x reauthentication

Operands None

Defaults Reauthentication is disabled.

Command Modes Interface subtype configuration mode

Description Use this command to enable 802.1X reauthentication on a port.

Usage Guidelines Enter **no dot1x reauthentication** to return to the default setting.

Examples To enable 802.1X reauthentication on a specific 10-gigabit Ethernet interface port:

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

To disable 802.1X reauthentication on a specific 1-gigabit Ethernet 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 802.1X reauthentication.

Synopsis **dot1x reauthMax** *number*
 no dot1x reauthMax

Operands *number* Specifies the maximum number of reauthentication attempts before the port goes to the unauthorized state. Valid values range from 1 through 10.

Defaults The number of times that a port attempts 802.1X authentication is 2.

Command Modes Interface subtype configuration mode

Description Use this command to set the maximum number of times that a port attempts to reauthenticate before a port changes to the unauthorized state.

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

Examples To set the maximum number of reauthentication attempts to 5 on a specific 10-gigabit Ethernet 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 40-gigabit Ethernet 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** *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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 monitor 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 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 Ten Gigabit
Ethernet1/0/13 is EAPOL capable.
```

See Also None

dot1x test timeout

Sets the 802.1X readiness test timeout.

Synopsis **dot1x test timeout** *timeout*

Operands *timeout* Specifies the interval value in seconds. Valid values range from 1 through 65535.

Defaults 10 seconds

Command Modes Global configuration mode

Description Use this command to set the 802.1X readiness test timeout.

Usage Guidelines None

Examples To set the test timeout to 30 seconds:
 `switch(config)# dot1x test timeout 30`

See Also **dot1x test eapol-capable**

dot1x timeout re-authperiod

Sets the 802.1X reauthorization-attempts interval.

Synopsis **dot1x timeout re-authperiod** *seconds*
 no dot1x timeout re-authperiod

Operands *seconds* Specifies the seconds between reauthorization attempts. Valid values range from 1 through 4294967295 seconds.

Defaults 3600 seconds

Command Modes Interface subtype configuration mode

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

Usage Guidelines Enter **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 1-gigabit Ethernet 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 40-gigabit Ethernet 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 the 802.1X authentication-server 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 802.1X authentication server. Valid values range from 1 through 65535.

Defaults 30 seconds

Command Modes Interface subtype configuration mode

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

Usage Guidelines Enter **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 10-gigabit Ethernet 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 1-gigabit Ethernet 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 for 802.1X authentication.

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. Valid values range from 1 through 65535.

Defaults 30 seconds

Command Modes Interface subtype configuration mode

Description Use this command to set 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 Enter **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 10-gigabit Ethernet 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 40-gigabit Ethernet 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 between successive request ID attempts. Valid values range from 1 through 65535 seconds.

Defaults 30 seconds

Command Modes Interface subtype configuration mode

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

Usage Guidelines Enter **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 10-gigabit Ethernet 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 40-gigabit Ethernet 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

<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies the slot number.
<i>port</i>	Specifies the port number.
reserve	Reserves a POD assignment for a port that is currently not able to come online but is expected to be viable in the future. A port license assignment that is reserved will be associated with the first port set that has a vacancy.
release	Removes a port from the port set to which it is currently assigned.

Defaults None

Command Modes Global configuration mode

Description Use this command to manage Dynamic POD assignments.

Usage Guidelines A port POD assignment can only be released if the port is currently offline. Enter **shutdown** to take the port offline.

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 Brocade VDX 6710 and Brocade VDX 8770 switches. 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`

dscp-cos

Specifies a user-defined mutation-map to be used on the port.

Synopsis **dscp-cos** *map_name*

Operands *map_name* The user-defined map-name.

Defaults None

Command Modes Policy-map configuration mode

Description Use this command to specify a user-defined mutation-map to be used on the port.

Usage Guidelines This command is allowed only for the Ingress direction.

This command can only be configured in for the **class class-default** command.

This command can lead to a possible contradiction if there are other user-defined classes used in the same policy-map which has a set CoS action configured. In this case, defined CoS takes priority over the mutation map.

Examples Typical command example:

```
switch(config)# policy-map mutation  
switch(config-policymap)# class class-default  
switch(config-policyclass)# dscp-cos plsmap
```

See Also **class**, **policy-map**

dscp-mutation

Specifies the dscp-mutation mutation-map to be used on the port.

Synopsis **dscp-mutation** *map_name*

Operands *map_name* The user-defined map-name.

Defaults None

Command Modes Policy-map configuration mode-

Description Use this command to specify the dscp-mutation mutation-map to be used on the port.

Usage Guidelines This command is allowed only for the ingress direction.

This command can only be configured in for the **class class-default** command.

This command can lead to a possible contradiction if there are other user-defined classes used in the same policy-map which has a set cos action configured. In this case-defined cos takes priority over the mutation map.

Examples Typical command example:

```
switch(config)#policy-map mutation  
switch(config-policymap)#class class-default  
switch(config-policyclass)# dscp-mutation plsmap
```

See Also **class**, **policy-map**

dscp-traffic-class

Specifies the traffic-class mutation-map to be used on the port.

Synopsis **dscp-traffic-class** *map_name*

Operands *map_name* The user-defined map-name.

Defaults None

Command Modes Policy-map configuration mode

Description Use this command to specify the traffic-class mutation-map to be used on the port.

Usage Guidelines This command is allowed only for the ingress direction.

This command can only be configured in for the **class class-default** command.

This command can lead to a possible contradiction if there are other user-defined classes used in the same policy-map which has a set cos action configured. In this case-defined cos takes priority over the mutation map.

Examples Typical command example:

```
switch(config)#policy-map mutation  
switch(config-policymap)#class class-default  
switch(config-policyclass)# dscp-traffic-class plsmap
```

See Also **class**, **policy-map**

ebs

Optional command for configuring the excess burst size of a class-map.

Synopsis **ebs** *ebs-size*
 no ebs *ebs-size*

Operands *ebs-size* Excess burst size. Valid values range from 1250 through 5000000000 bytes in increments of 1 byte.

Defaults None

Command Modes Policy-map class police configuration mode

Description This command configures the excess burst size of a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples This example configures a class-map called "default" within a policy-map.

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# ebs 400000
```

See Also **cbs, conform-set-dscp, conform-set-prec, conform-set-tc, eir, exceed-set-dscp, exceed-set-prec, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy, set-priority**

eir

Optional command for configuring the excess information rate for a class-map.

Synopsis **eir** *eir-rate*
 no eir *eir-rate*

Operands *eir-rate* Excess information rate. Valid values range from 0 through 40000000000 bps in multiples of 40000.

Defaults None

Command Modes Policy-map class police configuration mode

Description This command configures the excess information rate for a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples This example configures a class-map called "default" within a policy-map.

```
switch# configure terminal
switch(config)# policy-map policemap1
switch(config-policemap)# class default
switch (config-policemap-class)# police cir 40000
switch(config-policemap-class-police)# eir 800000
```

See Also **cbs, conform-set-dscp, conform-set-prec, conform-set-tc, ebs, exceed-set-dscp, exceed-set-dscp, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy, set-priority**

hello-interval (ELD)

This global level configuration defines the interval for sending edge-loop detection (ELD) PDUs.

Synopsis **hello-interval** *milliseconds*
 no hello-interval *milliseconds*

Operands milliseconds Interval time in milliseconds.

Defaults The default value is 1000 ms (one second)

Command Modes ELD configuration mode

Description The range is from 100 ms through 5 seconds.

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

It is the user's responsibility to make sure that the hello interval is set to the same value across the various VCS clouds. Otherwise, the ELD port shutdown will be non-deterministic.

Extreme caution must be taken when setting the hello-interval value to anything less than 1 second, as it will heavily increase the cpu load due to the amount of packets transmitted and received (depending on the number of ELD instances and other system configuration), and might cause undesirable performance and scalability results.

Enter **no hello-interval** *milliseconds* to return to the default setting.

Examples To set the PDU hello-interval to 5 seconds:

```
switch(config)# protocol edge-loop-detection
switch(config-eld)# hello-interval 5000
```

To return the PDU hello-interval to the default value (1000 ms):

```
switch(config-eld)# no hello-interval 5000
```

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 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. Valid values range from 0 through 256; a higher number indicates a lower priority.

Defaults ELD priority is 128.

Command Modes Interface subtype configuration mode

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.

NOTE

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.

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

Enter **no edge-loop-detection port-priority** to return to the default setting.

Examples To set the ELD priority of a specific 10-gigabit Ethernet 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 40-gigabit Ethernet 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 (ELD) on a port and VLAN.

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

Operands **vlan** *vlan-ID* Specifies a VLAN. (Refer to the Usage Guidelines.)t.

Defaults Edge-loop detection is disabled.

Command Modes Interface subtype configuration mode

Description Use this command to enable edge-loop detection for a specific VLAN ID.

Usage Guidelines Use the VLAN parameter 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.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

This command applies to Brocade VCS Fabric mode only.

This functionality detects Layer 2 loops only.

Enter **no edge-loop-detection vlan** *vlan_id* to disable edge-loop detection on the specified VLAN.

Examples To enable edge-loop detection on VLAN 10 for a specific 10-gigabit Ethernet 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 1-gigabit Ethernet interface 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**

enable statistics direction

Enables collection of statistics for tunnels.

Synopsis **enable statistics direction { tx | rx | both} vlan [add | remove] VLAN_ID_range**
no enable statistics

Operands

tx	Specifies the collecting of statistics for the transmitting tunnels.
rx	Specifies the collecting of statistics for the receiving tunnels.
both	Specifies the collecting of statistics for both the transmitting and receiving tunnels.
add	Enables statistics collecting on specified VLAN IDs. You can use this option if you have disabled specific VLAN IDs and now want to re-enable them.
remove	Disables statistics collecting on specified VLAN IDs.
VLAN_ID_range	Specifies the VLAN IDs for statistics reporting.

Defaults None

Command Modes VXLAN Gateway Configuration mode

Description This configuration enables per-VLAN statistics collection for the packets sent and received over the tunnels associated with this gateway instance.

If you remove all VLAN IDs from statistics collection, statistics collection becomes disabled and the *remove* option does not appear in the command line interface of this running configuration.

The only way to change the direction once you have run this command is to run the command **no enable statistics**, then rerun the command **enable statistics direction**.

Usage Guidelines The specified VLAN IDs must already be configured.

The **no** form of this command disables per-VLAN statistics collection for this gateway.

You cannot delete an attached VLAN if statistics collection is enabled on that VLAN.

Examples To enable statistics collecting for all tunnels in both directions for VLAN IDs 1 through 10:

```
switch# configure
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# enable statistics direction both vlan 1-10
```

See Also

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**

enable statistics direction

Enables collection of statistics for tunnels.

Synopsis **enable statistics direction { tx | rx | both} vlan [add | remove] VLAN_ID_range**
no enable statistics

Operands	tx	Specifies the collecting of statistics for the transmitting tunnels.
	rx	Specifies the collecting of statistics for the receiving tunnels.
	both	Specifies the collecting of statistics for both the transmitting and receiving tunnels.
	add	Enables statistics collecting on specified VLAN IDs. You can use this option if you have disabled specific VLAN IDs and now want to re-enable them.
	remove	Disables statistics collecting on specified VLAN IDs.
	VLAN_ID_range	Specifies the VLAN IDs for statistics reporting.

Defaults None

Command Modes VXLAN Gateway Configuration mode

Description This configuration enables per-VLAN statistics collection for the packets sent and received over the tunnels associated with this gateway instance.

If you remove all VLAN IDs from statistics collection, statistics collection becomes disabled and the *remove* option does not appear in the command line interface of this running configuration.

The only way to change the direction once you have run this command is to run the command **no enable statistics**, then rerun the command **enable statistics direction**.

Usage Guidelines The specified VLAN IDs must already be configured.

The **no** form of this command disables per-VLAN statistics collection for this gateway.

You cannot delete an attached VLAN if statistics collection is enabled on that VLAN.

Examples To enable statistics collecting for all tunnels in both directions for VLAN IDs 1 through 10:

```
switch# configure
switch(config)# overlay-gateway gateway1
switch(config-overlay-gw-gateway1)# enable statistics direction both vlan 1-10
```

See Also

enable

Enables a VRRP-E session.

Synopsis **enable**
 no enable

Operands None

Defaults None

Command Modes Virtual-router-group configuration mode

Description Use this command to enable a VRRP-E session.

Usage Guidelines Use the **no** form of this command to disable a VRRP-E session.

Examples To enable a VRRP-E session on VRRP-E group 10 on interface Ve 25:

```
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)# enable
```

See Also **vrrp-group, vrrp-extended-group**

enforce-first-as (BGP)

Enforces the use of the first autonomous system (AS) path for external BGP (EBGP) routes.

Synopsis **enforce-first-as**
 no enforce-first-as

Operands None

Defaults This option is disabled.

Command Modes BGP configuration mode

Description Use this command to enforce the first AS path, causing the router to discard updates received from EGBP peers that do not list their AS number as the first AS path segment in the AS_PATH attribute of the incoming route.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To configure the device to enforce the use of the first AS path:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# enforce-first-as
```

See Also None

enodes-config

Configures the number of FCoE interfaces to be created on FCoE nodes (ENodes).

Synopsis **enodes-config** [**global** | **local**]

no enodes-config

Operands **global** The value set by the **fcoe-enodes** command on all nodes in the cluster is changed on all RBridges in the cluster to the maximum of all values set by the **fcoe-enodes** command. (Refer to the Usage Guidelines.)

local Refer to the Usage Guidelines.

Defaults The default is **local**.

Command Modes RBridge ID configuration mode, fabric map configuration mode

Description Use this command to configure the number of FCoE interfaces to be created on ENodes.

Usage Guidelines In previous Network OS releases, the number of Virtual Fabric ports was configured globally on all switches in a VCS cluster.

With the option set to **global**, the value set by the **fcoe-enodes** command on all nodes in the cluster is changed on all RBridges in the cluster to the maximum of all values set by the **fcoe-enodes** command. The number of additional FCoE interfaces created is the difference between the value set by the **max-enodes** command and the value set by the **fcoe-enodes** command. The value of **max-enodes** is set to the maximum of the value set by the **fcoe-enodes** command, with a default of 256.

The option must be set to **global** for the system to downgrade from Network OS v4.1.0 or later to Network OS v4.0.0. The values set by the **max-enodes** command or the **fcoe-enodes** command are not modified; once the **global** option is executed, you cannot modify the value of **fcoe-enodes** in an RBridge context, or the value of **max-enodes** in a global context.

Following an upgrade to Network OS v4.1.0 or later, the default is set to **local**. With the option set to **local**, a downgrade is not allowed.

Use the **no** form of this command to restore the default.

Examples To configure the device to enable a downgrade to the previous Network OS release, execute the **fabric-map default** command in RBridge ID configuration mode, then issue the **enodes-config global** command:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# fabric-map default
switch(config-rbridge-id-10-fcoe-fabric-map)# enodes-config global
```

To return to the default setting, issue either of the following commands:

```
switch(config-rbridge-id-10)# no enodes-config
switch(config-rbridge-id-10)# enodes-config local
```

See Also **fcoe-enodes**, **max-enodes**

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 configuration 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.

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.

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 time for the interface to time out. Valid values range from 10 through 1000000 seconds.

Defaults 300 seconds
 The timeout feature is disabled.

Command Modes Protocol Spanning Tree configuration mode

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

Usage Guidelines If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.
 Enter **no error-disable-timeout interval** to return to the default setting.

Examples To set the timeout value to 10 seconds:
 switch(conf-rstp) # **error-disable-timeout interval 10**

See Also **error-disable-timeout enable**

exceed-set-dscp

Optional command for configuring the CIR packet IP precedence of a class-map.

Synopsis **exceed-set-dscp** *dscp-num*
 no exceed-set-dscp *dscp-num*

Operands *dscp-num* 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 *dscp-num* variable. Valid values are 0 through 7.

Defaults None

Command Modes Policy-map class police configuration mode

Description This command configures the CIR packet IP precedence of a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples Example of setting this parameter.

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# exceed-set-dscpc 4
```

See Also **cbs, conform-set-dscp, conform-set-prec, conform-set-tc, ebs, eir, exceed-set-prec, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy, set-priority**

exceed-set-prec

Optional command for configuring the CIR packet IP precedence of a class-map.

Synopsis **exceed-set-prec** *prec-num*
 no exceed-set-prec *prec-num*

Operands *prec-num* 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. Valid values are 0 through 7.

Defaults None

Command Modes Policy-map class police configuration mode

Description This command configures the CIR packet IP precedence of a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples Example of setting this parameter.

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# exceed-set-prec 4
```

See Also **cbs, conform-set-dscp, conform-set-prec, conform-set-tc, ebs, eir, exceed-set-dscp, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy, set-priority**

exceed-set-tc

Optional command for configuring the queue assignment of the *trafficclass* variable for a class-map.

Synopsis **exceed-set-tc** *trafficclass*
 no exceed-set-tc *trafficclass*

Operands *trafficclass* 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. Valid values are 0 through 7.

Defaults None

Command Modes Policy-map class police configuration mode

Description This command configures the queue assignment of the *trafficclass* variable for a a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples Example of setting this parameter.

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)# exceed-set-tc 4
```

See Also **cbs, conform-set-dscp, conform-set-prec, conform-set-tc, ebs, eir, exceed-set-dscp, exceed-set-prec, police cir, police-priority-map, policy-map, qos cos, service-policy, set-priority**

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.

Usage Guidelines When used in EXEC and Privileged EXEC modes, the **exit** command terminates the session.

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, enable**

external-lsdb-limit (OSPF)

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

Synopsis **external-lsdb-limit** *value*
 no external-lsdb-limit

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

Defaults 14913080

Command Modes OSPF VRF router configuration mode

Description Use this command to configure 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 Enter **no external-lsdb-limit** to return to the default setting.

Examples To set the limit of the LSDB to 20000:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# external-lsdb-limit 20000
```

See Also **database-overflow-interval (OSPF)**

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 Use this command to configure the list of fields (in the incoming packets), used for hashing.

Usage Guidelines This command does not function in standalone mode.

Examples To set 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. Valid values range from 0x0 through 0xFFFFFFFF.

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command 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 ISL ports are enabled persistently.

Command Modes Interface subtype configuration mode

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.

Enter **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 10-gigabit Ethernet 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 40-gigabit Ethernet 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

fabric neighbor-discovery disable

Disables neighbor discovery for Brocade devices on a per-interface basis.

Synopsis **fabric neighbor-discovery disable**
 no fabric neighbor-discovery

Operands None

Defaults Neighbor discovery is enabled by default.

Command Modes Interface subtype configuration mode

Description Use this command to disable neighbor discovery for Brocade devices on a specified interface.

Usage Guidelines This command functions in Brocade VCS Fabric mode only.
 Use the **no** form of this command to reenable neighbor discovery on this interface.

Examples To disable neighbor discovery on a specified tengigabitethernet interface:

```
switch# configure
switch(config)# interface tengigabitethernet 1/0/18
switch(config-if-te-1/0/18)# fabric neighbor-discovery disable
```

See Also None

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 RBridge ID. This is not valid in standalone mode.
 rbridge-id Specifies the RBridge ID.
 priority Sets a priority. The highest priority overrides the lowest RBridge ID and becomes the root.
 priority Specifies the priority number of the RBridge.

Defaults 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.

Command Modes Interface subtype configuration mode

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.

ISLs are not allowed on breakout ports.

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

NOTE

Trunks are not supported between Brocade 8000 and Brocade VDX 8770 switches.

Examples To enable a port for trunking on a specific 10-gigabit Ethernet 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 40-gigabit Ethernet 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 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. Refer to the Description.

Defaults The default flavor is src-dst-ip-mac-vid-port.

Command Modes RBridge ID configuration mode

Description Use this command to configure the load balancing feature on a remote RBridge which is not a member of the vLAG (also known as a nonlocal 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 below.

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 FCoE fabric-map configuration mode.

Synopsis **fabric-map default**

Operands None

Defaults None

Command Modes FCoE configuration mode

Description Use this command to enable the FCoE fabric-map configuration 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**

fast-external-failover (BGP)

Resets the session if a link to an EBGp peer goes down.

Synopsis **fast-external-failover**
 no fast-external-failover

Operands None

Defaults This option is disabled.

Command Modes BGP configuration mode

Description Use this command to terminate and reset external BGP sessions of an directly adjacent peer if the link to the peer goes down, without waiting for the timer, set by the BGP **timers** command, to expire.

Usage Guidelines This can improve BGP conversion time, but can also lead to instability in the BGP routing table as a result of a flapping interface.

Use the **no** form of this command to restore the default.

Examples To configure the device to reset the session if a link to an EBGp peer goes down:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# fast-external-failover
```

See Also **timers (BGP)**

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. Valid values range from 0E:FC:00 through 0E:FC:FF.

Defaults The FPMA FCMAP 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 Use this command to enable the FCoE configuration mode, allowing configuration of FCoE.

Usage Guidelines None

Examples `switch(config)# fcoe`
 `switch(config-fcoe)#`

See Also **fcoe, fabric-map**

fcoe-enodes

Sets the number of FCoE ENodes that are to be created on a switch.

Synopsis **fcoe-enodes** *number*
no fcoe-enodes

Operands *number* The number of FCoE interfaces. The range is from 0 through 1000.

Defaults The default value is 64.

Command Modes RBridge ID configuration mode, fabric map configuration mode

Description Use this command to set the number of FCoE ENodes that are to be created on a switch.

Usage Guidelines This command replaces the **max-enodes** command.

If the user tries to configure the number of FCoE interfaces with the above command, an error is thrown as in the following example:

```
switch(config)# fcoe
switch(config-fcoe)# fabric-map default
switch(config-fcoe-fabric-map)# max-enodes 500
%Error: This command is not allowed to configure max enodes. Please use
fcoe-enodes under rbridge mode.
```

This feature requires an FCoE license. If that license is not present, the number of FCoE ENodes created is 0. When that license is removed, it is recommended that the switch be rebooted. The number of FCoE ENodes created is set to 0 and all interfaces are deleted.

Examples To set the number of FCoE ENodes to be created to 67:

```
switch(config)# rbridge-id 10
sw0(config-rbridge-id-10)# fcoe
sw0(config-rbridge-fcoe)# fabric-map default
sw0(config-rbridge-fcoe-fabric-map)# fcoe-enodes 67
2013/08/16-09:59:11, [FCOE-1035], 9267, DCE, INFO, sw0, Virtual FCoE port 1/19/65
is online.
2013/08/16-09:59:11, [FCOE-1035], 9268, DCE, INFO, sw0, Virtual FCoE port 1/19/66
is online.
2013/08/16-09:59:11, [FCOE-1035], 9269, DCE, INFO, sw0, Virtual FCoE port 1/19/67
is online.
sw0(config-rbridge-id-19-fcoe-fabric-map)#
```

See Also **fabric-map**, **enodes-config**

fcoe-profile (AMPP)

Activates the FCoE profile configuration mode for AMPP.

Synopsis **fcoe-profile**

Operands None

Defaults None

Command Modes Port-profile configuration mode

Description Use this command to activate the FCoE profile configuration mode for AMPP. This allows configuration of the FCoE attributes of a port-profile.

Usage Guidelines The only fcoe-profile name allowed is “default”.

Examples `switch(config)# port-profile default`
 `switch(config-port-profile-default)# fcoe-profile`
 `switch(config-fcoe-profile)# fcoeport default`

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 subtype configuration mode

Description Use this command to configure a specific port to be an FCoE port with the assigned map name **default**.

Usage Guidelines The only map name allowed is **default**.
Enter **no fcoeport** to remove the FCoE port configuration from the applicable port.

Examples To provision a specific 10-gigabit Ethernet 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	
	RBridge ID 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.	
After 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.		

Authentication policy configuration is not distributed across the cluster. The rbridge-id of the node should be used to configure protocol and policy configurations.

Examples Standalone mode

To set 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
```

VCS mode

NOTE

This command is not distributed across the cluster. The RBridge ID of the node should be used to configure protocol and policy configurations.

To set only the authentication type:

```
switch(config)# rbridge-id 3  
switch(config-rbridge-id-3)# fcsp auth auth-type dh-chap
```

To set only the hash type:

```
switch(config)# rbridge-id 2  
switch(config-rbridge-id-2)# fcsp authhashsha1
```

To activate the device authentication policy:

```
switch(config)# rbridge-id 2  
switch(config-rbridge-id-2)# fcsp authpolicy switch active
```

See Also **fcsp auth-secret dhchap, show fcsp auth-secret dh-chap, show running-config fcsp auth**

fcsp auth-secret dhchap

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.

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 only supported on Brocade VDX 6730 switches.
 Enter **no fcsp auth-secret dhchap node** *switch_wwn* to remove the DHCHAP authentication secrets from the data base, so that the switch with the given WWN cannot connect to the local switch.

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# no fcsp auth-secret dh-chap 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 Gbps 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 **fill-word** value is **idle-idle**.

Command Modes Interface Fibre Channel configuration mode

Description Use this command to configure the link initialization and fill word for an 8 Gbps Fibre Channel port. By default, this command disables and re-enables the port and the port comes online with the new fill word setting.

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.

This command should be left at the default setting unless the remote port requires a specific setting for fill word.

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**

filter-change-update-delay

Sets a delay to change the delay in the filter-change status prompt from the default.

Synopsis **filter-change-update-delay** *delay_time*
 no filter-change-update-delay

Operands *delay_time* The delay, in seconds, in the filter-change status prompt. Range is from 0 through 600.

Defaults The default value is 10.

Command Modes RBridge ID configuration mode

Description Use this command to change the delay in the filter-change status prompt from the default.

Usage Guidelines Enter 0 (zero) or use the **no** form of this command to disable the timer.

Examples None

See Also None

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	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. Refer to the <i>Network OS Administrator's Guide</i> 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 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. Refer to 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	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. Refer to the <i>Network OS Administrator's Guide</i> 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: <pre>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</pre>
See Also	fips selftests, fips root disable, prom-access disable, show prom-access, unhide fips

firmware activate

Activates the firmware in the Local or remote nodes after installing the firmware that was downloaded with **firmware download noactivate** selected.

Synopsis **firmware activate** [**rbridge-id** {*rbridgeid_1-rbridgeid_3*, *rbridgeid_5*} | **all**]

Operands **rbridge-id** Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id Specifies a unique identifier for a node. Values can be a range of nodes or individual nodes and are separated by a comma.

all Specifies all identifiers for a node. The command applies to all of the nodes.

Defaults Activation of the firmware is performed manually by default after a download.

Command Modes Privileged EXEC mode

Description Reboots (activates) the switch after a firmware upgrade.

In a switch, this command will swap the CF partitions, reboot the system, and commit the new firmware on the CF partitions.

In a chassis, this command will swap the CF partition in both management modules, reboot the standby management module, forcing an HA failover on the active management module, download firmware to all line cards, and then commit firmware on all management modules and line cards.

If firmware activate is set to **noactive** with the **firmware download** command, firmware will be loaded to secondary partitions of both management modules and to all line cards without auto activating.

If firmware activate is set with the **firmware download** command, the firmware is activated on all nodes.

Usage Guidelines After firmware has been upgraded on a node, the firmware must be activated.

The **rbridge-id** operand is supported in VCS mode only.

Examples Standalone mode

To activate firmware on a switch:

```
switch# firmware activate
This command will use the ISSU protocol to upgrade the system. It will cause a
WARM reboot and will require that existing telnet, secure telnet or SSH sessions
be restarted.
Do you want to continue? [y/n]: y
```

```
2010/01/29-23:48:35, [HAM-1004], 226, switchid 1, CHASSIS | VCS, INFO,
Brocade_Elara2, Switch will be rebooted with the new firmware.
```

VCS mode

To activate firmware on switch nodes 1, 2, 3, and 5:

```
switch# firmware activate rbridge-id rid1-rid3,rid5
```

See Also firmware download, firmware restore, show version, show firmwaredownloadstatus

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** parameter set for the following **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 { default-config ftp scp sftp usb interactive } [manual] [nocommit] [noreboot] [noactivate] host { <i>hostname</i> <i>host_ip_address</i> } user <i>username</i> password <i>password</i> directory <i>directory</i> [file <i>file_name</i>] [vcs-mode <i>vcs mode</i>] [vcs-id <i>vcs ID</i>] [rbridge-id <i>rbridge ID</i>]]	
Operands	default-config	Sets the configuration back to default except for the following parameters: VCS mode, VCS ID, and RBridge ID. These three parameters are retained except when the options to change their values are specified.
	ftp scp sftp usb	Valid protocols are ftp (File Transfer Protocol) or scp (Secure Copy), sftp (SSH File Transfer Protocol), usb (universal serial bus). The values are not case-sensitive.
	interactive	Runs firmware download in interactive mode. You are prompted for input.
	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 parameter 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.
	noactivate	Downloads the firmware to the system without activating it.
	host	Specifies the host by DNS name or IP address.
	<i>hostname</i>	Specifies an IPv4 DNS host name.
	<i>host_ip_address</i>	Specifies the host IP address. IPv4 and IPv6 addresses are supported.
	directory <i>directory</i>	Specifies a fully qualified path to the directory where the firmware is located.
	file <i>file_name</i>	Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.
	user <i>username</i>	Specifies the user login name for the host.
	password <i>password</i>	Specifies the account password.
	vcs-mode <i>vcs mode</i>	Specifies the new VCS mode. If not set, the existing VCS mode is used. It is only available in local firmware download.
	vcs-id <i>vcs ID</i>	Specifies the new VCS ID. If not set, the existing VCS ID is used. It is only available in local firmware download.
	rbridge-id <i>rbridge ID</i>	Specifies the new RBridge ID. If not set, the existing RBridge ID is used. It is only available in local firmware download.
Defaults	firmware download performs an auto-reboot and a subsequent auto-commit operation.	

By default, **firmware download** downloads the firmware to the system, reboots the system, and commits the firmware automatically. The user can specify **noactivate** to download the firmware to the system without activating it (the node is not rebooted). The user can run **firmware activate** later to activate the firmware.

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.

When **default-config** is specified, the VCS mode, VCS ID and RBridge ID options will be displayed. In a dual-MM system, if you specify the **manual** option with the **default-config** option, make sure you execute the same command on both MM. After firmware download is completed on both MM, *you must reboot them at the same time*. Otherwise, the MM may run into configuration mismatch issues.

Examples In logical chassis cluster mode, you have the option to download firmware to multiple nodes:

```
switch# firmware download interactive
Do you want to download to multiple nodes in the cluster? [y/n]: y
Server name or IP address:
```

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 to a local node:

```
switch# firmware download protocol ftp host 10.1.2.30 user fvt password  
pray4green path /dist file release.plist
```

This command will download the firmware to the local node. You will need to run `firmware activate` to activate the firmware after this command completes.

Do you want to continue? [y/n]: y

```
2010/01/29-23:48:35, [HAM-1004], 226, switchid 1, CHASSIS | VCS, INFO,  
Brocade_switch,  
Firmwaredownload has started on the switch.
```

To download firmware using the **default-config** option with VCS mode 1, VCS ID 7, and RBridge 10, use the following command:

```
sw0# firmware download default-config ftp host 10.20.1.3 user fvt password  
pray4green directory dist file release.plist vcs-mode 1 vcs-id 7 rbridge-id 10
```

Performing system sanity check...

This command will set the configuration to default and set the following parameters: vcs-mode, vcs-id and rbridge-id.

This command will cause Cold reboot on both MMs at the same time and will require that existing telnet, secure telnet or SSH sessions be restarted.

Do you want to continue? [y/n]: y

```
host 10.20.1.3 user fvt password pray4green directory dist file release.plist
```

Performing system sanity check...

This command will set the configuration to default and set the following parameters: vcs-mode, vcs-id and rbridge-id.

This command will cause Cold reboot on both MMs at the same time 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, show firmwaredownloadstatus, show version**

firmware download ftp

Specifies FTP as the protocol used to perform a firmware download.

Synopsis **firmware download ftp** [**coldboot**] [**manual**] [**nocommit**] [**noreboot**] **host** {*hostname* | *host_ip_address*} **user** *username* **password** *password* **directory** *directory* [**file** *file_name*] [**noactivate**]

Operands	coldboot	Performs a non-ISSU firmware download. When firmware is downloaded onto a chassis system, it is sometimes necessary to specify the coldboot option. This option must be specified on the active MM only. When specified, the coldboot option downloads firmware onto both the active and standby MMs at the same time. After the firmware completes downloading on both MMs, they are rebooted at the same time. This ensures that both MMs reboot with the same firmware, and prevents any firmware compatibility issues that may exist between the old and the new firmware.
		Caution: Do not use this option unless instructed to do so by Brocade Technical Support.
	directory <i>directory</i>	Specifies a fully qualified path to the directory where the firmware is located.
	file <i>filename</i>	Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.
	host	Specifies the host by DNS name or IP address.
	<i>hostname</i>	Specifies an IPv4 DNS host name.
	<i>host_ip_address</i>	Specifies the host IP address. IPv4 and IPv6 addresses are supported.
	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 parameter is ignored when issued on a compact switch or in a chassis with only one management module.
	noactivate	Performs a firmware download without activation on the local switch.
	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.
	password <i>password</i>	Specifies the account password.
	user <i>username</i>	Specifies the user login name for the host.
Defaults	firmware download performs an auto-reboot and a subsequent auto-commit operation.	

By default, **firmware download** downloads the firmware to the system, reboots the system, and commits the firmware automatically. The user can specify **noactivate** to download the firmware to the system without activating it (the node is not rebooted). The user can run **firmware activate** later to activate the firmware.

Command Modes Privileged EXEC mode

Description Use this command to download firmware from an external host.

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 None

See Also **firmware commit**, **firmware restore**, **show firmwaredownloadstatus**, **show version**

firmware download interactive

Allows the user to select firmware download parameters interactively before starting a firmware download.

Synopsis **firmware download interactive**

Operands None

Defaults **firmware download** performs an auto-reboot and a subsequent auto-commit operation.

By default, **firmware download** downloads the firmware to the system, reboots the system, and commits the firmware automatically.

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 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 parameters:

```
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, sftp): ftp
User: fvt
Password: *****
Do manual download [y/n]: n

System sanity check passed.

Do you want to continue? [y/n]: y
```

See Also **firmware commit**, **firmware restore**, **show firmwaredownloadstatus**, **show version**, **firmware download**

firmware download logical-chassis

Downloads the firmware onto the switches.

Synopsis **firmware download logical-chassis** default-config {ftp | scp | sftp} host *host_ip* user *username* password *password* path *path* [*rbridge-id* *rbridgeid_1-rbridgeid_3*, *rbridgeid_5* | all] [auto-activate]

Operands

default-config	Sets the configuration back to default except the following parameters: VCS mode, VCS ID, and RBridge ID. These three parameters are retained.
ftp	Specifies FTP as the protocol used to download the firmware.
scp	Specifies SCP as the protocol used to download the firmware.
sftp	Specifies SFTP as the protocol used to download the firmware.
host <i>host_ip</i>	Specifies the host IP address.
user <i>username</i>	Specifies the username.
password <i>password</i>	Specifies the password.
path <i>path</i>	Specifies the filename path where the firmware is located.
auto-activate	Specifies to automatically activate the firmware on the switches after installing the firmware.
rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
<i>rbridge-id</i>	Specifies a unique identifier for a node. Values can be a range of nodes or individual nodes and are separated by a comma.
all	Specifies all identifiers for a node.

Defaults After firmware is downloaded to the nodes, the command returns without rebooting the nodes. You will need to run **firmware activate** to active the new firmware on the nodes.

Command Modes Privileged EXEC mode

Description Downloads the firmware onto the switch.

Usage Guidelines The command is controlled by a principal node (coordinator) and executed on individual nodes in the VCS cluster. All sanity check error and warning messages are displayed on the coordinator user session. If an error results during the Installation, the firmware download request is aborted.

Examples To activate firmware on switch nodes 1, 2, 3, and 5:

```
switch# firmware activate rbridge-id rid1-rid3,rid5
```

To perform a firmware recovery on all switch nodes:

```
switch# firmware recover rbridge-id all
```

To automatically activate firmware on switch nodes rbridge-id 161 and 62 when in logical chassis cluster mode:

```
switch# firmware download logical-chassis scp host 10.31.2.25 user release user
password releaseuser directory /pub/sre/SQA/nos/nos4.0.0/nos4.0.0_bld42
auto-activate rbridge-id 161,62
```

2 firmware download logical-chassis

To reboot switches in a specific order, which can be done from any node:

```
switch# firmware download logical-chassis rbridge-id all path path.  
firmware activate rbridge-id 2  
firmware activate rbridge-id 3  
firmware activate rbridge-id 4  
firmware activate rbridge-id 1
```

To download firmware using the **default-config** option, use the following command:

```
sw0# firmware download logical-chassis default-config ftp host 10.1.2.30 user fvt  
password brocade directory /dist/nos/4.0.0bld01 file release.plist rbridge-id  
1,2-3
```

Rbridge-id	Sanity Result	Current Version
1	Disruptive	4.1.0
2	Disruptive	4.1.0
3	Disruptive	4.1.0

You are invoking firmware download with the provision option. This command will download the new firmware to the specified nodes, default their configuration, and reboot them automatically.

Do you want to continue? [y/n]: y

See Also **firmware activate, firmware recover, show version, show firmwaredownloadstatus**

firmware download scp

Specifies SCP as the protocol used to perform a firmware download.

Synopsis **firmware download scp** [**coldboot**] [**manual**] [**nocommit**] [**noreboot**] **host** {*hostname* | *host_ip_address*} **user** *username* **password** *password* **directory** *directory* [**file** *file_name*] [**noactivate**]

Operands	coldboot	Performs a non-ISSU firmware download. When firmware is downloaded onto a chassis system, it is sometimes necessary to specify the coldboot option. This option must be specified on the active MM only. When specified, the coldboot option downloads firmware onto both the active and standby MMs at the same time. After the firmware completes downloading on both MMs, they are rebooted at the same time. This ensures that both MMs reboot with the same firmware, and prevents any firmware compatibility issues that may exist between the old and the new firmware.
		Caution: Do not use this option unless instructed to do so by Brocade Technical Support.
	manual	Performs a firmware download on the local switch.
	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. (Skips auto-commit after firmware download.)
	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.
	<i>hostname</i>	Specifies an IPv4 DNS host name.
	<i>host_ip_address</i>	Specifies the host IP address. IPv4 and IPv6 addresses are supported.
	user <i>username</i>	Specifies the user login name for the host.
	password <i>password</i>	Specifies the account password.
	directory <i>directory</i>	Specifies a fully qualified path to the directory where the firmware is located.
	file <i>file_name</i>	Specifies the firmware .plist file. This parameter is optional.
	noactivate	Performs a firmware download without activation on the local switch.

Defaults A filename is optional. If no filename is specified, release.plist, is used.

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.

2 firmware download scp

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

None

See Also

firmware commit, firmware restore, show firmwaredownloadstatus, show version

firmware download sftp

Specifies SFTP as the protocol used to perform a firmware download.

Synopsis **firmware download sftp** [**coldboot**] **directory** *directory* [**manual**] [**nocommit**] [**noreboot**] **host** {*hostname* | *host_ip_address*} **user** *username* **password** *password* **directory** *directory* [**file** *file_name*] [**noactivate**]

Operands	coldboot	Performs a non-ISSU firmware download. When firmware is downloaded onto a chassis system, it is sometimes necessary to specify the coldboot option. This option must be specified on the active MM only. When specified, the coldboot option downloads firmware onto both the active and standby MMs at the same time. After the firmware completes downloading on both MMs, they are rebooted at the same time. This ensures that both MMs reboot with the same firmware, and prevents any firmware compatibility issues that may exist between the old and the new firmware.
	Caution:	Do not use this option unless instructed to do so by Brocade Technical Support.
	directory <i>directory</i>	Specifies a fully qualified path to the directory where the firmware is located.
	file <i>filename</i>	Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.
	host	Specifies the host by DNS name or IP address.
	<i>hostname</i>	Specifies an IPv4 DNS host name.
	<i>host_ip_address</i>	Specifies the host IP address. IPv4 and IPv6 addresses are supported.
	manual	Performs a firmware download on the local switch.
	no activate	Performs a firmware download without activation on the local switch.
	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. (Skips auto-commit after firmware download.)
	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.
	password <i>password</i>	Specifies the account password.
	user <i>username</i>	Specifies the user login name for the host.

Defaults None

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.

2 firmware download sftp

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

None

See Also

firmware commit, firmware restore, show firmwaredownloadstatus, show version

firmware download usb

Specifies USB as the protocol used to perform a firmware download.

Synopsis `firmware download usb [coldboot] [noactivate] [nocommit] [noreboot] [manual] directory directory`

Operands **coldboot** Performs a non-ISSU firmware download. When firmware is downloaded onto a chassis system, it is sometimes necessary to specify the coldboot option. This option must be specified on the active MM only. When specified, the coldboot option downloads firmware onto both the active and standby MMs at the same time. After the firmware completes downloading on both MMs, they are rebooted at the same time. This ensures that both MMs reboot with the same firmware, and prevents any firmware compatibility issues that may exist between the old and the new firmware.

Caution: Do not use this option unless instructed to do so by Brocade Technical Support.

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

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 parameter is ignored when issued on a compact switch or in a chassis with only one management module.

noactivate Performs a firmware download without activation on the local switch.

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.

Defaults None

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.

2 firmware download usb

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

```
switch# firmware download usb directory NOS_v3.0.0
```

See Also **firmware commit, firmware restore, show firmwaredownloadstatus, show version**

firmware install

Installs new software but deletes all configuration in the system.



CAUTION

Do not use this command unless instructed by Brocade Technical Support.

synopsis	firmware install {ftp scp} host <i>host_ip_address</i> user <i>username</i> password <i>password</i> ddirectory <i>directory</i> [file <i>file_name</i>] [vcs-mode {0 1 2}] [vcs-id <i>vcs_id</i>] [rbridge-id <i>rbridge ID</i>]	
Operands	ftp	Specifies FTP as the protocol used to install the firmware.
	scp	Specifies SCP as the protocol used to install the firmware.
	host	Specifies the host by DNS name or IP address.
	<i>host_ip_address</i>	Specifies the host IP address. IPv4 and IPv6 addresses are supported.
	user <i>username</i>	Specifies the user login name for the host.
	password <i>password</i>	Specifies the account password.
	directory <i>directory</i>	Specifies a fully qualified path to the directory where the firmware is located.
	file <i>filename</i>	Specifies the firmware .plist file. This parameter is optional; if unspecified, the default file, release.plist, is used.
	[vcs-mode {0 1 2}]	Specifies the VCS mode for the switch when the new firmware has been installed. If not set, the platform-dependent default VCS mode is used. Values you can select are: 0 (fabric cluster mode), 1 (logical chassis cluster mode), or 2 (standalone mode).
	vcs-id <i>vcs_id</i>	Specifies the new VCS ID when the new firmware has been installed. If not set, the platform-dependent default VCS ID is used. Range is 1 to 8192.
	rbridge-id <i>rbridge ID</i>	Specifies the new Rbridge ID when the new firmware has been installed. If not set, the platform-dependent default Rbridge ID is used. Range is 1 to 239.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	This command cleans the existing firmware on the system before installing the new firmware. All configurations in the system is completely lost.	

2 firmware install

Usage Guidelines	• In a dual-MM system, after firmware install is completed on both MM's, reboot them at the same time. Otherwise, the MM's may run into configuration mismatch issue. • If vcs-id or rbridge-id are specified, vcs-mode cannot be set to 2 (standalone). • On the Brocade 8770, 6740, 6740T, and 6740T-1G, vcs-mode cannot be set to 2 (standalone). • If you want to change vcs-mode from standalone to either fabric cluster mode or logical chassis cluster mode, you must use both the vcs-id and rbridge-id options with this command. • If you specify at least one of the vcs-mode, vcs-id or rbridge-id parameters, then the remaining parameters will get their values from the existing configuration — unless you also specify their values in the command line.
Examples	To install new firmware, delete all existing configurations, and to specify the vcs mode, vcs ID and RBridge ID you want the switch to come up in: <pre>switch# firmware install scp host 10.70.4.109 user fvt pass pray4green directory /buildsjc/sre/SQA/nos/nos4.1.0/nos4.1.0_bld25 vcs-mode 1 vcs-id 6 rbridgeid 10</pre>
See Also	None

firmware recover

Recovers the previous firmware version on the switch nodes if a firmware upgrade was unsuccessful.

Synopsis `firmware recover [rbridge-id {rbridge-id_1-rbridge-id_3, rbridge-id_5 | all}]`

Operands

rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
<i>rbridge-id</i>	Specifies a unique identifier for a node. Values can be a range of nodes or individual nodes and are separated by a comma.
all	Specifies all identifiers for a node. The command applies to all of the nodes. The command applies to all of the nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Allows you to undo the operation that was performed using the firmware download “noactivate” option.

If you invoke a noactivate firmware download, the firmware is loaded to the secondary node without swapping partitions. If firmware recover is executed, it will perform a forceful commit in that node. This CLI does not reboot the node.

Usage Guidelines The **rbridge-id** operand is supported in VCS mode only.

Examples To recover firmware on switch nodes 1, 2, 3, and 5:

```
switch# firmware recover rbridge-id rid1-rid3,rid5
```

To perform a firmware recovery on all switch nodes:

```
switch# firmware recover rbridge-id all
```

See Also `firmware activate`, `show version`, `show firmwaredownloadstatus`

firmware restore

Swaps the partition and reboots the node.



CAUTION

Do not use this command unless instructed by Brocade Technical Support.

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. This command causes the node to boot up with its older firmware. Later, the image in the primary partition is automatically committed to the secondary partition.
Usage Guidelines	This command is supported only on the local management module. The firmware download command must have been run with the nocommit parameter for the firmware restore operation to succeed.
Examples	To restore the previous firmware: <pre>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 ...</pre>
See Also	firmware commit, firmware download, show version

firmware sync

Synchronizes firmware to standby MM.

Synopsis **firmware sync**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Run this command from the active MM to sync the firmware version on the standby MM to the version on the active MM. After the firmware is copied to the standby MM, the standby MM automatically reboots, after which the firmware takes effect.

Usage Guidelines None

Examples None

See Also None

forward-delay

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

Synopsis **forward-delay** *seconds*
 no forward-delay

Operands *seconds* Specifies the time that an interface spends in the Spanning Tree Protocol (STP) learning and listening states. Valid values range from 4 through 30 seconds.

Defaults 15 seconds

Command Modes Protocol Spanning Tree configuration 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.

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:

$$2 * (\text{forward-delay} - 1) \geq \text{max-age} \geq 2 * (\text{hello-time} + 1)$$

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.

Enter **no forward-delay** to return to the default settings.

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

```
switch(config-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. Both 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 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. Failover and reboots can be disruptive.

Examples To perform an HA reboot:

```
switch# ha chassisreboot
```

See Also **ha failover, ha enable, reload, show ha**

ha disable

Disables the High Availability feature.

Synopsis **ha disable**

Operands None

Defaults HA is 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 This command is supported only on the active management module.
This command is not supported on the standby management module.
Do not use this command unless instructed by Brocade Technical Support.

NOTE

With the introduction of Network OS 4.0, failover is no longer disruptive for Layer 2.

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, reload, show ha**

ha enable

Enables the High Availability feature.

Synopsis **ha enable**

Operands None

Defaults HA is 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.

Running the command displays a warning message and prompts for confirmation before rebooting the management module.

You can also use this command to display the servers that are running the syslogd daemon and those that system messages are sent to. Servers are specified in the configuration database by IP address.

Usage Guidelines This command is supported only on the local management module.

This command is not supported on the standby management module.

Do not use this command unless instructed by Brocade Support.

NOTE

With the introduction of Network OS 4.0, failover is no longer disruptive for all Layer 2.

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, reload, show ha**

ha failover

Initiates a failover from the active to the standby management module (MM).

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 MM. When the process completes, the former standby takes over as the active MM. If the active and standby MMs are not synchronized, the command aborts.
Usage Guidelines	With the introduction of Network OS 4.0, failover is no longer disruptive for all Layer 2. The following summarizes the behavior of the ha failover command under a variety of conditions. The modes are as follows:

Mode	Definition
FC	Fabric Cluster. In FC mode, the data path for nodes is distributed, but the configuration path is not distributed. Each node maintains its own configuration database. This command causes a warm recovery.
LC	Logical chassis cluster. In LC mode, both the data path and the configuration path are distributed. This command causes a cold recovery.

Behavior of the **ha failover** command

HA synchronized		HA not synchronized	
Active	Standby	Active	Standby
Reboots the active MM.	In FC mode, there is a warm recovery on the standby MM. In MC mode there is always a cold recovery.	Not allowed.	Not allowed.

Examples	To perform a failover: <pre>switch# ha failover</pre>
See Also	ha failover, ha enable, ha sync start, ha sync stop, reload, show ha

ha sync start

This command is used to enable the high availability (HA) state synchronization.

Synopsis **ha sync start**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description After an **ha sync stop** command has been invoked, use the **ha sync start** command to enable HA state synchronization.

Usage Guidelines None

Examples To enable HA synchronization:

```
switch# ha sync start
Are you sure you want to start sync [y/n]
All service instances in sync
2012/10/06-16:10:36, [HASM-1100], 630, M2, INFO, VDX8770-4, HA State is in sync.
```

See Also **ha failover, ha enable, ha disable, ha sync stop, show ha**

ha sync stop

Disables high availability state synchronization on a switch.

Synopsis **ha sync stop**

Operands None

Defaults Synchronization is enabled.

Command Modes Privileged EXEC mode

Description Use this command to disable state synchronization.

Usage Guidelines None

Examples To disable state synchronization:

```
switch# ha sync stop
```

```
Are you sure you want to stop sync [y/n]? y
```

```
Service instances out of sync
```

```
2012/10/06-16:06:13, [HASM-1101], 619, M2, WARNING, VDX8770-4, HA State out of sync.
```

See Also **ha failover, ha enable, ha sync start**

hardware

Enters hardware configuration mode to enter connector and port-group configuration mode.

Synopsis **configure hardware**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to enter hardware configuration mode. While in this mode you can enter connector configuration mode for the purpose of configuring breakout mode. You can also enter port-group configuration mode on Brocade 27x40 GbE line cards.

Usage Guidelines None

Examples switch# **config**
switch(config)# **hardware**
switch(config-hardware)#

See Also **exit, connector, sfp breakout, port-group**

hello (LLDP)

Sets the Hello transmit interval.

Synopsis **hello** *seconds*
no hello

Operands *seconds* Valid values range from 4 through 180 seconds.

Defaults 30 seconds

Command Modes LLDP protocol configuration mode

Description Use this command to set the interval between LLDP hello messages.

Usage Guidelines Enter **no hello** to return to the default setting.

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

```
switch# configure terminal
switch (config)# protocol lldp
switch(config-lldp)# hello 10
```

See Also None

hello (UDLD)

Sets the hello transmit interval.

Synopsis **hello** *hundred_milliseconds*
no hello

Operands *hundred_milliseconds* Valid values range from 1 through 60 (in counts of 100 milliseconds).

Defaults 5 is the default value (500 milliseconds).

Command Modes Unidirectional link detection (UDLD) protocol configuration mode

Description Use this command to set the time interval between the transmission of hello UDLD PDUs from UDLD-enabled ports.

Usage Guidelines Enter **no hello** to return to the default setting.

Examples To set the time interval to 2,000 milliseconds between hello UDLD PDU transmissions:

```
switch# configure  
switch (config)# protocol udld  
switch(config-udld)# hello 20
```

See Also **protocol udld, multiplier (UDLD)**

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

Operands *interval* Number of periods between each PDU. For example, a value of 2000 causes a PDU to be sent every two seconds. Valid values range from 100 through 5000 milliseconds (100 ms through 5 seconds).

Defaults 1000 (one second)

Command Modes ELD configuration mode

Description Use this command to set the interval between PDU packets sent from the ELD-enabled edge ports of a Brocade VCS Fabric cluster.

Usage Guidelines 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.

This command applies only in Brocade VCS Fabric mode.

This functionality detects Layer 2 loops only.

Enter **no hello-interval** to return to the default setting.



CAUTION

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*

no hello-time

Operands *seconds* Specifies the time interval between the hello BPDUs sent on an interface. Valid values range from 1 through 10 seconds.

Defaults 2 seconds

Command Modes Protocol Spanning Tree configuration 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.

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.

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:

$$2 * (\text{forward-delay} - 1) \geq \text{max-age} \geq 2 * (\text{hello-time} + 1)$$

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.

Enter **no hello-time** to return to the default settings.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples

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

```
switch(conf-stp) # hello-time 5
```

See Also **forward-delay**, **max-age**

hello-timer

Configures the Hello message periodic interval.

Synopsis **hello-timer** *num*
 no hello-timer

Operands *num* The interval value in seconds. Valid values range from 10 through 3600 seconds.

Defaults 30 seconds

Command Modes PIM router configuration mode

Description Use this command to specify the interval between Protocol Independent Multicast (PIM) “Hello” messages.

Usage Guidelines Enter **no hello-timer** to return to the default settings.

Examples Setting the hello-timer to 60 seconds.

 `switch(conf-pim-router)# hello-timer 60`

See Also **router pim**

hold-time

Sets the time that a previously down backup VRRP router, which also must have a higher priority than the current master VRRP router, will wait before assuming mastership of the virtual router.

Synopsis **hold-time** *range*

Operands *range* A value between 1 and 3600 seconds that specifies the time a formerly down backup router waits before assuming mastership of the virtual router.

Defaults 0 seconds

Command Modes Virtual-router-group configuration mode

Description Use this command to set 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 0 seconds 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**

http server shutdown

Disables or enables an HTTP server.

Synopsis **http server shutdown**
 no http server shutdown

Operands None

Defaults None

Command Modes Global configuration mode

Description Use this command to disable or enable an HTTP server.

Usage Guidelines Use the **http server shutdown** command to disable an HTTP server. All active connections are closed and the Apache httpd server process does not run.

 Use the **no http server shutdown** command to enable an HTTP server. This restarts the Apache httpd server process, which starts listening for HTTP requests.

ATTENTION

You cannot downgrade directly to a previous Network OS release with the HTTP server disabled. You must first execute the **no http server shutdown** command and then downgrade.

Examples To disable an HTTP server:

```
switch(config)# http server shutdown
```

 To enable an HTTP server:

```
switch(config)# no http server shutdown
```

See Also None

inactivity-timer

Configures the forwarding entry inactivity timer.

Synopsis **inactivity-timer** *num*
 no inactivity-timer

Operands *num* The entry inactivity timer interval. Valid values range from 60 through 3600 seconds.

Defaults 180 seconds

Command Modes PIM router configuration mode

Description Use this command to specify the delay interval until a forwarding entry is considered to be active. At the expiration of this timer, the router deletes a forwarding entry.

Usage Guidelines Enter **no inactivity-timer** to return to the default setting.

Examples To set the timer to 600 seconds.

 switch(conf-pim-router)# **inactivity-timer 600**

See Also router pim

install-igp-cost (BGP)

Configures the device to use the IGP cost instead of the default BGP4 Multi-Exit Discriminator (MED) value as the route cost when the route is added to the Routing Table Manager (RTM).

Synopsis	install-igp-cost no install-igp-cost
Operands	None
Defaults	This option is disabled.
Command Modes	BGP configuration mode
Description	By default, BGP4 uses the BGP MED value as the route cost when the route is added to the RTM. Use this command to change the default to the IGP cost.
Usage Guidelines	Use the no form of this command to restore the default.
Examples	To configure the device to compare MEDs: <pre>switch(config)# rbridge-id 10 switch(config-rbridge-id-10)# router bgp switch(config-bgp-router)# install-igp-cost</pre>
See Also	None

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. Valid values range from 1 through 31.

vlan *vlan_id* Specifies the VLAN to map an MSTP instance. Refer to the Usage Guidelines.

priority *priority_id* Specifies the priority for the specified instance. Valid values range from 0 through 61440. The priority values can be set only in increments of 4096.

Defaults The priority value is 32768.

Command Modes Protocol Spanning Tree MSTP configuration mode

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

Usage Guidelines If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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.

Enter **no instance** to un-map the VLAN from the MSTP instance.



CAUTION

This command can be used only after the VLAN is defined.

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 <i>rbridge-id/slot/port</i> fcoe <i>vn-number/rbridge-id/front-port-number</i> fortygigabitethernet <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i> hundredgigabitethernet <i>rbridge-id/slot/port</i> port-channel <i>number</i> tengigabitethernet <i>rbridge-id/slot/port</i> vlan <i>vlan_id</i>] no interface [port-channel <i>number</i> vlan <i>vlan_id</i> fcoe <i>vn-number/rbridge-id/front-port-number</i>]
Operands	fibrechannel <i>rbridge-id/slot/port</i> Specifies a valid Fibre Channel port interface (Brocade VDX 6730 switches only in Brocade VCS Fabric mode). <i>rbridge-id</i> Specifies the RBridge ID. This is not valid in standalone mode. <i>slot</i> Specifies a valid slot number. <i>port</i> Specifies a valid port number. fcoe <i>vn-number/rbridge-id/front-port-number</i> Specifies a valid FCoE port interface. <i>vn-number</i> Specifies the VN number for FCoE. <i>rbridge-id</i> Specifies the routing bridge ID. This is not valid in standalone mode. <i>front-port-number</i> Specifies the front port number. fortygigabitethernet <i>rbridge-id/slot/port</i> Specifies a valid 40-gigabit Ethernet interface. <i>rbridge-id</i> Specifies the RBridge ID. This is not valid in standalone mode. <i>slot</i> Specifies a valid slot number. <i>port</i> Specifies a valid port number. gigabitethernet <i>rbridge-id/slot/port</i> Specifies a valid 1-gigabit Ethernet interface (Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches only). <i>rbridge-id</i> Specifies the RBridge ID. This is not valid in standalone mode. <i>slot</i> Specifies a valid slot number. <i>port</i> Specifies a valid port number. hundredgigabitethernet <i>rbridge-id/slot/port</i> Specifies a valid 100-gigabit Ethernet interface (Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches only). <i>rbridge-id</i> Specifies the RBridge ID. This is not valid in standalone mode. <i>slot</i> Specifies a valid slot number. <i>port</i> Specifies a valid port number. port-channel <i>number</i> Specifies the port-channel number. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.

tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
vlan <i>vlan_id</i>	Specifies the VLAN number. Refer to the Usage Guidelines.

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 switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

The **fibrechannel** *rbridge-id/slot/port* parameter is used only on 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* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches. The prompt for configuring these ports is in the following format:

```
switch(config-if-gi-22/0/1)#
```

Enter **no interface** followed by the appropriate interface identification parameters to disable that interface.

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-1/0/1)#
```

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 (range specification)

Allows a range of values to be entered for some interface configurations.

Synopsis	interface { fibrechannel <i>rbridge-id/slot/port</i> fcoe <i>vn-number/rbridge-id/front-port-number</i> fortygigabitethernet <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i> hundredgigabitethernet <i>rbridge-id/slot/port</i> port-channel <i>number</i> tengigabitethernet <i>rbridge-id/slot/port</i> vlan <i>vlan_id</i> loopback <i>port_number</i> ve <i>vlan_id</i> } no interface { port-channel <i>number</i> vlan <i>vlan_id</i> fcoe <i>vn-number/rbridge-id/front-port-number</i> }	
Operands	fibrechannel <i>rbridge-id/slot/port</i>	Specifies a valid Fibre Channel port interface (Brocade VDX 6730 switches only in Brocade VCS Fabric mode).
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	fcoe <i>vn-number/rbridge-id/front-port-number</i>	Specifies a valid FCoE port interface.
	<i>vn-number</i>	Specifies the VN number for FCoE.
	<i>rbridge-id</i>	Specifies the routing bridge ID. This is not valid in standalone mode.
	<i>front-port-number</i>	Specifies the front port number.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface (Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches only).
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	hundredgigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 100-gigabit Ethernet interface (Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches only).
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.

port-channel <i>number</i>	Specifies the port-channel number. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
vlan <i>vlan_id</i>	Specifies the VLAN number. (Refer to the Usage Guidelines.)
loopback <i>port_number</i>	Specifies the port number for the loopback interface. The range is 1 through 255.
ve <i>vlan_id</i>	Specifies the corresponding VLAN interface that must already be configured before the VE interface can be created. (Refer to the Usage Guidelines.)

Defaults None

Command Modes Global configuration mode (Refer to the Usage Guidelines.)

Description Use this command to create or enter the interface configuration mode for an interface or range of interfaces.

Usage Guidelines Loopback and VE configurations are in global configuration mode in stand alone mode, but are node specific (local) in fabric cluster and logical chassis cluster modes. The other interfaces that support the use of ranges work the same as shown for VLAN in the examples, except for the following differences:

VE and loopback interfaces also support ranges in RBridge configuration mode.

For example, if you want to create and/or enter VLAN interface configuration mode for VLAN IDs 3 through 8 and VLAN 10 and 12, you would enter the following command in global configuration mode:

```
switch(config)# interface vlan 3-8,10,12
```

NOTE

Do not use a space after a comma or you will receive a syntax error.

You then receive the following prompt:

```
switch(config-Vlan-3-8,10,12)#
```

Any command you run from this prompt takes effect on all VLANs that you have specified.

You can use the **no** form of commands on ranges in the same way. For example, if you want to remove the description on VLANs 10 through 15 and VLAN 19 all at the same time, you would enter the following commands in global configuration mode:

```
switch(config)# interface vlan 10-15,19
switch(config-vlan-10-15,19)# no description
```

NOTE

The **no** form of the command for deleting interfaces should not be given from the range sub-mode. Exit the range sub-mode before deleting interfaces.

The three gigabit interface types have the following restrictions for range specification in VCS mode:

- Ranges cannot be used for interfaces that belong to multiple slots. However, you can configure a range of interfaces if each interface in the range belongs to the same slot.
- Ranges can be applied only to interfaces that belong to the same RBridge.

Fibrechannel interfaces have the following restrictions for range specification in VCS mode:

- Ranges cannot be used for interfaces that belong to multiple slots. However, you can configure a range of interfaces if each interface in the range belongs to the same slot.
- Ranges can be applied only to interfaces that belong to the same RBridge.

For the fibre channel interface, ranges can be applied only to interfaces that belong to the same RBridge.

An FCoE interface from one node cannot be combined with a bind configuration of a physical port/port-channel that belongs to another node in the cluster. Refer to the Examples.

A set of FCoE ports cannot be bound to the same MAC address. On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples FCoE example

To configure binding between a range of FCoE ports (0 to 20 in this example) to the tengigabitethernet port 10/0/1:

```
switch# configure
switch(config)# interface Fcoe 1/10/0 - 1/10/20
sw0(conf-Fcoe-1/10/0-20) bind te 10/0/1
```

The FCoE interfaces and the bind configuration of the physical port/port-channel must belong to the same node in the cluster. An example of an unsupported configuration is:

```
switch# configure
switch(config)# interface Fcoe 1/10/0 - 1/10/20
sw0(conf-Fcoe-1/10/0-20) # bind te 20/0/1
```

Tengigabitethernet example for VCS mode

To enter interface subtype configuration mode on a tengigabitethernet interface with an RBridge ID of 25 and a slot of 0, with a port range of 1 through 10, 17 through 21, and 24:

```
sw0(config)# interface TenGigabitEthernet 25/0/1-10,17-21,24
sw0(conf-if-te-25/0/1-10,17-21,24)#
```

Tengigabitethernet example for standalone mode

To enter interface subtype configuration mode on a tengigabitethernet interface with a slot of 0, for a port range of 1 through 10, and 17 through 21:

```
sw0(config)# interface TenGigabitEthernet 0/1-10,17-21  
sw0(conf-if-te-0/1-10,17-21)#
```

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 through 255.

Defaults None

Command Modes RBridge ID configuration 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 Enter **no interface loopback** *port_number* to remove the specified loopback interface.

Example This example shows the steps needed to create a loopback interface with a port number of 25 for RBridge ID 11. 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

Enters configuration mode for the management interface. Also used for binding ACLs to a management interface.

Synopsis `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 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.

Defaults DHCP is disabled.
IPv6 stateless auto-configuration is disabled.
The speed setting is **auto**.

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.

Once you have executed this command, the following commands become available to configure the management interface:

- **ip address**
- **ip access-group**
- **ip gateway-address** (Refer to the Usage Guidelines.)
- **ip route**
- **ipv6 address**
- **ipv6 access-group**
- **speed**

Usage Guidelines The **ip gateway-address** command will not be available on the Brocade VDX series if the Layer 3 or Advanced Services license is installed. In that case, use the following command sequence:

```
switch(config)# rbridge-id 1
switch(config-rbridge-id-1)# ip route 0000/0 <default_gateway_address>
```

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.

A static IPv6 address and stateless auto-configuration can coexist.

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.

Enter **no ip address ipv4_address/prefix_len dhcp** to disable DHCP. For other operands, use the **no** form of the command to remove the corresponding configuration.

Enter **no speed** to restore speed parameters to their defaults.

2 interface management

Examples

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 a 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
```

Applying an ACL on management interface 1/1:

```
switch(config)# interface management  
switch(config)# interface management 1/1  
Entering configuration mode terminal  
switch(config-Management-1/1)# ip access-group stdACL1 in
```

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

interface ve

Configures a virtual Ethernet (VE) 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. Refer to the Usage Guidelines.

Defaults None

Command Modes RBridge ID configuration mode (for VCS)
 Global configuration mode (for standalone)

Description Use this command to configure a virtual Ethernet (VE) 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 Enter **no interface ve** *vlan_id* to remove the VE interface. This will not remove the corresponding VLAN interface.



CAUTION

If no RBridge ID is configured on the switch, deleting the VE interface will cause a spike in CPU usage. To prevent this, configure an RBridge ID before deleting the VE interface.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples The following example shows the steps needed to create a VE interface with the VLAN ID of 56 for RBridge ID 11. This example is for a VCS environment, and assumes that the VLAN 56 interface has already been created.

```
switch(config)# rbridge-id 11
switch(config-rbridge-id-11)# int ve 56
```

See Also interface; interface vlan

interface vlan

Allows the user to create 802.1Q VLANs, as well as service or transport VFs in a Virtual Fabrics context.

Synopsis **interface vlan** *vlan_id*
no interface vlan *vlan_id*

Operands *vlan_id* Specifies the VLAN interface to configure. The range is from 1 through 8191. (Refer to the Usage Guidelines.)

Defaults VLAN 1 is predefined on the switch.

Command Modes Global configuration mode

Description Use this command to configure a VLAN interface. This command applies to both 802.1Q VLANs (whose VLAN IDs range from 1 through 4095) and service or transport VFs (whose VLAN IDs range from 4096 through 8191). To support multitenancy, assigning VLAN IDs from 4096 through 8191 creates service or transport VFs that are unique within a local VCS Fabric but that cannot extend to another VCS Fabric.

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.

For service or transport VFs to be implemented in a Virtual Fabrics context, the user must execute the **vcs virtual-fabric enable** command in global configuration mode.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Enter **no interface vlan** *vlan_id* to delete a VLAN interface. This will also delete the corresponding virtual Ethernet (VE) interface.

Examples To create a VLAN with an ID of 56:

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

To create a classified VLAN (with an ID from 4096 through 8191):

```
switch(config)# interface vlan 5000
switch(conf-if-vl-5000)#
```


See Also interface, interface ve, fcmapi, shutdown (STP), switchport, vcs virtual-fabric enable

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 No access lists are applied to the interface.

Command Modes Interface subtype configuration mode

Description Use this command to apply a IP ACL to a Layer 2, Layer 3, or a VE interface. You create the IP ACL by using the **ip 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, an error results.

Enter **no ip access-group** *name* to remove the IP ACL from the interface.

Examples To apply an ingress IP ACL named *ipacl2* on a specific 10-gigabit Ethernet 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 10-gigabit Ethernet 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**, **mac access-list extended**, **resequence access-list**

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] [seq number]`

`no [ip | ipv6] access-list {standard | extended} [name] [seq number]`

Operands

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 hyphen.

[seq | no seq] access list Specifies the sequence number of the access list. The number must be from 0 through 4294967290 (applies to both standard and extended ACLs).

Defaults None

Command Modes Global configuration mode

Description Use this command to create a standard or extended IP 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 redefined.

Enter **no ip access-list** or **no ipv6 access-list** 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)# exit
switch(config)# exit
switch#
```

See Also interface management, seq (extended IP ACLs), seq (standard IP ACLs),
show running-config interface management, show running-config ip access-list

ip address

Configures an IP address.

Synopsis **ip address** *ip-address/mask* [**secondary**] [{**ospf-ignore** | **ospf-active**}]

no ip address

Operands	<i>ip-address</i>	IP address.
	<i>mask</i>	Mask for the associated IP subnet. Valid values range from integers from 1 through 31. 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.
	ospf-ignore	Disables adjacency formation with OSPF neighbors and advertisement of the interface to OSPF.
	ospf-passive	Disables adjacency formation with OSPF neighbors but does not disable advertisement of the interface to OSPF.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to configure a primary or secondary IP address for a specific interface. You can also use this command to prevent OSPF from running on specified subnets.

Usage Guidelines 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 be configured before you configure a secondary IP address in the same subnet.

Enter **no ip address** to remove the configured static or DHCP address, resetting the address to 0.0.0.0/0.

Examples To configure a primary IP address on a specific 10-gigabit Ethernet 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 40-gigabit Ethernet 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 (range specification)**, **interface ve**

ip address (NSX controller configuration)

Configures IP address and port information for an NSX controller connection profile.

Synopsis `ip address ip-address [method {ssl | tcp} ] [port port_number]`

Operands `ip address ip-address` IP address of the NSX Controller cluster. Only IPv4 addresses are allowed. This address is used to open a connection to the NSX Controller for Open vSwitch Database Management Protocol (OVSDB) exchange.

method Specifies the connection method for this profile.

ssl Specifies that a Secure Sockets Layer connection will be used. This is the default connection method.

tcp Specifies that a transmission control protocol will be used.

port port_number Specifies the port number for the NSX controller. The range is 1-65535. The default 6632.

Defaults None

Command Modes NSX controller configuration mode

Description Use this command to create or update the IP address, port and connection method settings for an NSX controller connection profile.

Usage Guidelines This command is allowed for a switch that is in logical chassis cluster mode only. The VXLAN gateway must be in shutdown state.

Examples The following example shows how to enter NSX controller configuration mode for the already created NSX controller connection profile called *profile1*, then how to create the IP address, set the method to TCP, and designate the port of 25:

```
switch# configuration
switch(config)# nsx-controller profile1
switch(config-nsx-controller-profile1)# ip address 10.21.83.188 method tcp port
25
```

See Also

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.
 For 1-gigabit, 10-gigabit, and 40-gigabit Ethernet interfaces, the range of valid values is from 0 through 240 minutes. For virtual Ethernet interfaces, the range is from 0 through 35790 seconds.

Defaults **ip arp-aging-timeout** is enabled and set to 10 minutes.

Command Modes Interface subtype configuration mode

Description Use this command to configure how long an ARP entry stays in cache before the cache refreshes.

Usage Guidelines When a Brocade device places an entry in the ARP cache, the 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.

Enter **no ip arp-aging-timeout** command to disable aging so that entries do not age out.

Entering **ip arp-aging-timeout 0** also disables aging.

Examples To set the IP ARP aging timeout value to 100 minutes for a specific 10-gigabit Ethernet 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 40-gigabit Ethernet 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 as-path access-list

Configures an AS-path access control list (ACL).

Synopsis **ip as-path access-list** *string* [**seq** *seq-value*] [**deny** *regular-expression* | **permit** *regular-expression*]
no ip as-path access-list *string* [**seq** *seq-value*] [**deny** *regular-expression* | **permit** *regular-expression*]

Operands *string* ACL name.
 seq-value Sequence number as defined by the **seq** command.
 regular-expression A string inside quotes.

Defaults This option is disabled.

Command Modes RBridge ID configuration mode

Description Use this command to configure an AS-path ACL, and to specify the community name and whether to permit or deny traffic. This command accepts a regular expression that must be enclosed in quotes.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To create an AS-path ACL:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# ip as-path access-list seq 10 permit "myaspath"
```

See Also **seq**

ip community-list extended

Configures a community access control list (ACL), and specifies the community name and whether to permit or deny traffic, including through the use of a regular expression.

Synopsis **ip community-list extended** *community-list-name* (**deny** *string* | **permit** *string*) [**seq** *seq*]
 [**internet** | **local-as** | **no-advertise** | **no-export**]
no ip community-list extended *community-list-name*

Operands

<i>community-list-name</i>	Range is from 1 through 32 ASCII characters.
<i>string</i>	An ordered community-list regular expression.
<i>seq</i>	Sequence number. Range is from 1 through 65535.
internet	The Internet community.
no-export	Community of sub-ASs within a confederation. Routes with this community can be exported to other sub-ASs in the same confederation but not outside the confederation to other ASs or otherwise sent to EBGp neighbors.
local-as	Local sub-AS within the confederation. Routes with this community can be advertised only within the local sub-AS.
no-advertise	Routes with this community cannot be advertised to any other BGP4 devices at all.
<i>regular-expression</i>	A string enclosed in quotes.

Defaults This option is disabled.

Command Modes RBridge ID configuration mode

Description Use this command to configure a community access control list (ACL), and to specify the community name and whether to permit or deny traffic. Unlike a standard community list, this command does accept a regular expression as long as the string is enclosed in quotes.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To create an extended community list:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# ip community-list extended seq 10 permit
"mycommunity"
```

See Also seq, ip community-list standard

ip community-list standard

Configures a community access control list (ACL), and specifies the community number or type and whether to permit or deny traffic.

Synopsis **ip community-list standard** *community-list-name* {**deny** [*community-number* | *AA:NN*] | **permit** [*community-number*] [**seq** *seq-value*] [**internet** | **local-as** | **no-advertise** | **no-export**]}
no ip community-list standard *community-list-name*

Operands

<i>community-list-name</i>	Range is from 1 through 32 ASCII characters.
<i>community-number</i>	A community number. Range is from 1 through 4294967295.
<i>AA:NN</i>	Autonomous system number and network number, configured as 2-byte numbers separated by a colon.
<i>seq</i>	Sequence number. Range is from 1 through 65535.
internet	The Internet community.
no-export	Community of sub-ASs within a confederation. Routes with this community can be exported to other sub-ASs in the same confederation but not outside the confederation to other ASs or otherwise sent to EBGp neighbors.
local-as	Local sub-AS within the confederation. Routes with this community can be advertised only within the local sub-AS.
no-advertise	Routes with this community cannot be advertised to any other BGP4 devices at all.

Defaults This option is disabled.

Command Modes RBridge ID configuration mode

Description Use this command to configure a community access control list (ACL), and to specify the community name or type and whether to permit or deny traffic. A standard community list does not accept a regular expression.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To create a standard community list:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# ip community-list standard seq 10 permit local-as
```

See Also **seq**, **ip community-list extended**

ip dhcp relay address

Configures the IP DHCP Relay on a Layer 3 interface.

Synopsis **ip dhcp relay address** *ip-addr* [**use-vrf** *vrf-name*]

Operands *ip-addr* IPv4 address of the DHCP server where the DHCP client requests are to be forwarded.

use-vrf Use this option if the VRF where the DHCP server is located is different from the VRF of the interface where the client is connected.

vrf-name VRF name.

Defaults None

Command Modes Interface configuration mode

Description Configures the IP DHCP Relay on the switch Layer 3 interface using the IPv4 address of the DHCP server where the DHCP client requests are to be forwarded. You can configure the address on a virtual Ethernet (VE) or a physical GigabitEthernet, TenGigabitEthernet, or FortyGigabitEthernet interface.

Usage Guidelines Enter the command while in interface configuration mode for a VE or physical interface where you want to configure the IP DHCP Relay. Configure up to four DHCP server IP addresses per interface. Use the **no** version of this command to remove the IP DHCP Relay from the interface. If the **use-vrf** option is not used, it is assumed that the DHCP server and interface where the client is connected are on the same VRF.

Examples To configure an IP DHCP Relay address on a TenGigabitEthernet interface in standalone mode:

```
sw0(config)# interface TenGiga 2/3/1
sw0(config-if-te-2/3/1)# ip dhcp relay address 100.1.1.2
```

To configure an IP DHCP Relay address on a VE interface in standalone mode:

```
sw0(config)# interface ve 100
sw0(config-Ve-100)# ip dhcp relay address 100.1.1.2
```

To configure an IP DHCP Relay address on a VE interface in VCS mode:

```
switch(config)# rbridge-id 1
switch(config-rbridge-id-1)# interface ve 101
switch(config-Ve-101)# ip dhcp relay address 100.1.1.2
switch(config-Ve-101)# ip dhcp relay address 12.3.4.6
```

To configure an IP DHCP Relay address on an interface if the DHCP server is on a different VRF than the interface where the client connects:

```
switch# config
Entering configuration mode terminal
switch(config)# rbridge-id 2
switch(config-rbridge-id-2)# interface ve 103
switch(config-Ve-103)# ip dhcp relay address 3.1.2.255 use-vrf blue
```

See Also **show ip dhcp relay address interface**

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.

Command Modes Interface subtype configuration mode

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 Enter **no ip directed-broadcast** to disable IP directed broadcasts on a specific interface.

Examples To enable IP directed broadcasts on a specific 10-gigabit Ethernet 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 40-gigabit Ethernet 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 IP address of the primary and secondary name servers. IPv6 and IPv4 addresses are 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.
 Name servers can only be entered or removed one at a time. The newly entered name server will append to the existing name server.

NOTE

If a domain name is not configured by means of the **domain-name** operand, DNS configuration will not work and a warning message will appear.

Enter **no ip dns domain-name** *domain_name* to disable IP directed broadcasts for a specific domain.

Enter **no ip dns name-server** *ip_address_of_name_server* to disable IP directed broadcasts for a specific 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 echo-reply

Enables the generation of an Internet Control Message Protocol (ICMP) Echo Reply message.

Synopsis **ip echo-reply**
 no ip echo-reply

Operands None

Defaults None

Command Modes Global configuration mode

Description Use this command to enable the generation of an ICMP Echo Reply message.

Usage Guidelines This is an interface-specific configuration. The configuration is persistent across a switch reload.

Examples None

See Also None

ipv6 echo-reply

Enables the generation of an ICMPv6 Echo Reply message.

Synopsis **ipv6 echo-reply**
 no ipv6 echo-reply

Operand None

Defaults None

Command Modes Global configuration mode

Description Use this command to enable the generation of an ICMPv6 Echo Reply message. This command supports Joint Interoperability Test Command (JITC).

Usage Guidelines The configuration is persistent across switch reload and is an interface specific configuration.

Examples None

See Also None

ip http-server enable

Enables the HTTP server.

Synopsis **ip http-server enable**
 no ip http-server enable

Operands None

Defaults The HTTP server is disabled by default.

Command Modes Global configuration mode

Description Use this command to enable the HTTP server. Once enabled, the HTTP daemon starts without the need to reboot.

Usage Guidelines Use the **no ip http-server enable** command to disable the HTTP server. All active HTTP connections are closed, followed by a restart of the Apache server.

Examples None

See Also None

ip icmp rate-limit

Limits the rate at which Internet Control Message Protocol (ICMP) messages are sent on an IPv4 network.

Synopsis **ip icmp rate-limit** *milliseconds*
no ip icmp rate-limit

Operand *milliseconds* Number of milliseconds between packets. The range is from 1 through 4294967295.

Defaults The default value is 1000 milliseconds.

Command Modes Interface configuration mode

Description This command limits the rate at which ICMP messages are sent on an IPv4 network. To protect against TCP SYN attacks, you can configure the Brocade device to drop TCP SYN packets when excessive numbers of messages are encountered. You can set threshold values for TCP SYN packets that are targeted at the router itself or passing through an interface, and drop them when the thresholds are exceeded.

Usage Guidelines The configuration is persistent across a switch reload. Once it is enabled, all outbound ICMP message types are rate limited.

Examples None

See Also None

ipv6 icmp rate-limit

Limits the rate at which ICMP messages are sent on a IPv6 network.

Synopsis **ipv6 icmp rate-limit** *milliseconds*
no ipv6 icmp rate-limit

Operand *milliseconds* Number of milliseconds between packets. The range is from from 1 through 4294967295.

Defaults The default value is 1000 milliseconds.

Command Modes Interface configuration mode

Description This command limits the rate at which ICMP messages are sent on a IPv6 network. To protect against TCP SYN attacks, you can configure the Brocade device to drop TCP SYN packets when excessive numbers are encountered. You can set threshold values for TCP SYN packets that are targeted at the router itself or passing through an interface, and drop them when the thresholds are exceeded.

This command supports Joint Interoperability Test Command (JITC).

Usage Guidelines The configuration is persistent across switch reload.
 Once enabled, all outbound ICMP message types are rate limited.

Examples None

See Also ip icmp rate-limit

ip igmp immediate-leave

Removes a group from the IGMP table immediately when receiving a Leave Group request.

Synopsis **ip igmp immediate-leave**
 no ip igmp immediate-leave

Operands None

Defaults This command is disabled.

Command Modes VE interface configuration mode
 Router interface configuration mode

Description Use this command to treat the interface as if it had one multicast client, so receipt of a Leave Group request on the interface causes the group to be immediately removed from the multicast database.

Usage Guidelines Enter **no ip igmp immediate-leave** to restore the default setting.

Examples None

See Also None

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. Valid values range from 100 through 25500 milliseconds.

Defaults 1000 milliseconds

Command Modes VE interface configuration mode
 VLAN interface configuration mode
 Router interface configuration 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 Enter **no ip igmp last-member-query-interval** to remove the last-member query interval on a specific interface.

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**, **interface ve**, **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. Valid values range from 1 through 18000 seconds.

Defaults 125 seconds

Command Modes VE interface configuration mode
 VLAN interface configuration mode
 Router interface configuration mode

Description Use this command to set the query interval. This is the amount of time between IGMP query messages sent by the switch.

Usage Guidelines Enter **no ip igmp query-interval** to remove the query interval on a specific interface.

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. Valid values range from 1 through 25 seconds.

Defaults 10 seconds

Command Modes VE interface configuration mode
 VLAN interface configuration mode
 Router interface configuration 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 Enter **no ip igmp query-max-response-time** to restore the default maximum response time for IGMP queries.

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.

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.

Enter **no ip igmp snooping enable** to return to the default setting.

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 configuration 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 Enter **no ip igmp snooping enable** 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, interface ve, 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 command is disabled.

Command Modes VLAN interface configuration mode

Description Use this command to enable Internet Group Management Protocol (IGMP) snooping fast-leave processing. This allows the removal of an interface from the forwarding table without sending out group-specific queries to the interface.

Usage Guidelines Enter **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, interface ve, 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** {**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 parameter to specify the interface.

fortygigabitethernet *rbridge-id/slot/port*
Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This 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-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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. Valid values range from 1 through 63 for standalone mode, and 1 through 6144 for Brocade VCS Fabric mode.

Defaults None

Command Modes VLAN interface configuration 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 On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Enter **no ip igmp snooping mrouter** to remove the configured mrouter.

This command is mutually exclusive of **ip igmp snooping querier enable**.

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 through 60000 seconds.

Defaults 300 seconds

Command Modes VLAN interface configuration mode

Description Use this command to set the timeout range for when multicast router ports are automatically learned on a specific VLAN interface.

Usage Guidelines Enter **no ip igmp snooping mrouter-timeout** to restore the default mrouter value of 300 seconds on the VLAN interface.

Examples To configure the mrouter timeout value to 600 seconds on a 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.

Command Modes VLAN interface configuration mode

Description Use this command to control the IGMP snooping querier functionality.

Usage Guidelines Enter **no ip igmp snooping querier enable** to disable the IGMP snooping querier.
This command is mutually exclusive of **ip igmp snooping mrouter interface**.

Examples To enable the IGMP snooping querier feature for the 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*
 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, 10.0.0.1), as the allowable range of addresses included in the multicast group.

Defaults None

Command Modes VE interface configuration mode
 VLAN interface configuration mode
 Router interface configuration mode

Description Use this command to 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 PIMmcache table.

Usage Guidelines Enter **no ip igmp static-group** *A.B.C.D* to restore the default setting for the specified group address.

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 225.1.1.1 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 225.1.1.1
```

See Also **interface**, **ip igmp last-member-query-interval**, **ip igmp query-interval**,
 ip igmp query-max-response-time

ip interface

Sets the IP address of the VXLAN overlay-gateway instance.

Synopsis **ip interface** *Ve veid* **vrrp-extended-group** *group-ID*
no ip interface

Operands *veid* Specifies the ID of the virtual ethernet interface (which must already be configured) through which you are configuring the IP address of the VXLAN gateway.

group-ID Specifies the virtual router group (which must already be configured) through which you are configuring the IP address of the VXLAN gateway.

Defaults None

Command Modes VXLAN Gateway Configuration mode

Description Use this command to set the IP address of the VXLAN overlay gateway. The command accepts the VE interface ID and VRPP-E group ID, then sets the overlay gateway IP address as identical to the already configured Virtual Redundancy Router Protocol-Extended (VRRP-E) virtual IP address.

Changing the VE interface ID or VRRPE group ID would require an update of all tunnel source addresses.

Usage Guidelines Be sure the VXLAN gateway is in the inactive state when you issue this command.

If you have already added Rbridge attachments to the VXLAN gateway overlay, the VE and VRPP-E group IDs must exist for the attached Rbridge IDs.

Use the **no** form of this command to delete the IP address configuration for this gateway.

Some commands cannot be used if they would affect an active VXLAN gateway address configuration. For example, consider the following configuration:

```
switch# configure
switch(config)# overlay-gateway xx
switch(config-overlay-gw-xx)# attach rbridge-id add 1
switch(config-overlay-gw-xx)# ip interface ve 1000 vrrp-extended-group 100
switch(config-overlay-gw-xx)# activate
```

Examples of operations that would not be allowed based on this configuration are:

- Deleting VLAN 1000 (because this implicitly deletes VE 1000)
- Deleting VE 1000 on Rbridge 1
- Deleting VRRP-E group 100 for VE 1000 on Rbridge 1
- Changing virtual IP configuration for VE 1000, VRRPE group 100 on Rbridge 1
- Changing VRF on VE 1000 on Rbridge 1

2 ip interface

Examples To set the IP address of a VXLAN gateway overlay named *gateway1* (using the already configured Ve interface ID 10 and the vrrp-extended group ID 25):

```
switch# configure  
switch(config)# overlay-gateway gateway1  
switch(config-overlay-gw-gateway1)# ip interface Ve 10 vrrp-extended-group 25
```

See Also

ip load-sharing

Enables load sharing.

Synopsis **ip load-sharing** *paths*
 no ip load-sharing

Operands *paths* Specifies the number of load-sharing paths. Valid values range from 0 to 8. The default is 8. If you specify 1, load sharing is disabled.

Defaults Load sharing is enabled and set to 8 paths.

Command Modes RBridge ID configuration mode

Description Use this command to enable load sharing and set the maximum number of load-sharing paths. By default, IP load sharing allows IP traffic to be balanced across up to 8 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 a Brocade device has six next-hop routers, you should set the maximum paths value to 6.

Usage Guidelines Enter **no ip load-sharing** to remove the load sharing configuration and restore the 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
```

See Also None

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.

Defaults MTU size is 1500 bytes.

Command Modes Interface subtype configuration mode

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.

The allowed MTU size is from 576 to 9018 bytes.

Enter **no ip mtu** to reset the MTU size to the default.

Examples To set the MTU size to 2000 bytes on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9  
switch(conf-if-te-178/0/9)# ip mtu 2000
```

See Also **interface**

ip multicast-boundary

Configures a multicast boundary on an interface.

Synopsis **ip multicast-boundary**
 no ip multicast-boundary

Operands None

Defaults No multicast boundaries are defined on an interface.

Command Modes Interface configuration mode

Description Use this command to configure a multicast boundary on an interface. Since there is no support for a prefix-list, this command applies the boundary for the entire multicast range on the interface.

Usage Guidelines Enter **no ip multicast-boundary** to disable this feature.

Examples None

See Also None

ip ospf active

Sets a specific OSPF interface to active.

Synopsis **ip ospf active**

Operands None

Defaults None

Command Modes Interface subtype configuration mode

Description Use the **ip ospf active** command to change the state to active on specific OSPF interfaces.

Usage Guidelines Use the **ip ospf active** command on each interface participating in adjacency formation. This command overrides the global passive setting on that interface, and enables transmission of OSPF control packets.

Examples To set a specific OSPF virtual Ethernet (VE) interface to active:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# int ve 100
sw0(config-Ve-100)# ip ospf active
```

See Also **ip ospf passive**

ip ospf passive

Sets a specific OSPF interface to passive.

Synopsis **ip ospf passive**

Operands None

Defaults None

Command Modes Interface subtype configuration mode

Description Use the **ip ospf passive** command to change the state on to passive on specific OSPF interfaces.

Usage Guidelines Use the **ip ospf passive** command to disable transmission of OSPF control packets on that interface. OSPF control packets received on a passive interface are discarded.

Examples To set a specific OSPF virtual Ethernet (VE) interface to passive:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# int ve 200
sw0(config-Ve-200)# ip ospf passive
```

See Also **ip ospf active**

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.

Defaults OSPF is disabled.

Command Modes Interface subtype configuration mode

Description Use this command to enable an OSPF area on the interface to which you are connected.

Usage Guidelines Enter **no ip ospf area** to disable OSPF on this interface.

Examples To enable a configured OSPF area named 0 on a specific OSPF 10-gigabit Ethernet 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 virtual Ethernet (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 before an authentication change takes place. Valid values range from 0 to 14400 seconds.

Defaults Wait time is 300 seconds

Command Modes Interface subtype configuration mode

Description Use this command to set or reset 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 Enter **no ip ospf auth-change-wait-time** to reset the wait time to the default of 300 seconds.

Examples To set the wait time to 600 seconds on a specific OSPF 10-gigabit Ethernet 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 virtual Ethernet (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 <i>password</i> as a plain text password and shows the unencrypted password in the show running command output as follows: <code>key 0 passwd</code>
2 password	Expects the user to provide the encrypted password, preceded by a dollar sign (\$) sign, and shows the encrypted password in the show running command output as follows: <code>key 2 \$c1pVT0=</code>
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: <code>key 2 \$c1pVT0=</code>
password	OSPF processes <i>password</i> 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: <code>key 2 \$c1pVT0=</code>

Defaults No authentication.

Command Modes Interface subtype configuration mode

Description Use this command to sets or reset simple password-based authentication on the OSPF interface to which you are connected.

Usage Guidelines Enter **no ip ospf authentication-key** to disable OSPF authentication.

Examples The following command sets authentication only on the OSPF 10-gigabit Ethernet 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(config-if-te-190/0/49)# ip ospf authentication-key brocade
```

The following example sets authentication on the OSPF virtual Ethernet (VE) interface 12, with 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. Valid values range from 1 through 65535.

Defaults Cost value is 1.

Command Modes Interface subtype configuration mode

Description Use this command to set or reset 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, refer to the **auto-cost reference-bandwidth (OSPF)** command.

Usage Guidelines Enter **no ip ospf cost** to disable this configuration.

Examples To set the cost to 600 on a specific OSPF 10-gigabit Ethernet 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 virtual Ethernet (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 (OSPF)**

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 }} no ip ospf database-filter all-external no ip ospf database-filter all-out no ip ospf database-filter all-summary-external	
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	Filters outgoing LSAs.
	all-out	Blocks all LSAs.
	all-summary-external	Blocks all summary (Type 3) and external (type 5) LSAs.
Defaults	All filters are disabled.	
Command Modes	Interface subtype configuration mode	
Description	Use this command to configure filters for different types of outgoing LSAs.	
Usage Guidelines	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. Enter no ip ospf database-filter followed by the appropriate operands to disable this configuration.	

NOTE
You cannot block LSAs on virtual links.

Examples To apply a filter to block flooding of all LSAs on a specific OSPF 40-gigabit Ethernet 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 virtual Ethernet (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.

Defaults The default value is 40 seconds.

Command Modes Interface subtype configuration mode

Description Use this command to set 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 Enter **no ip ospf dead-interval** to use the default value.

Examples To set the dead interval to 80 on a specific OSPF 40-gigabit Ethernet 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 virtual Ethernet (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 the hello interval.

Synopsis **ip ospf hello-interval** *interval*
no ospf hello-interval

Operands *interval* Hello interval in seconds.

Defaults The default value is 10 seconds.

Command Modes Interface subtype configuration mode

Description Use this command to set 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 Enter **no ospf hello-interval** to use the default value.

Examples To set the hello interval to 200 on a specific OSPF 40-gigabit Ethernet 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 virtual Ethernet (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 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. Valid values range from 0 to 14400 seconds. The default value is 300 seconds.

key-id

Sets MD5 key and OSPF password.

id MD5_key

The *num* is a number between 1 and 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 dollar sign (\$), and shows the encrypted password in the **show running** command output as follows:

```
key 2 $c1lpVT0=
```

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 $c1lpVT0=
```

ospf_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 $c1lpVT0=
```

Defaults No authentication.

Command Modes Interface subtype configuration mode

Description Use this command to sets or reset the MD5 password and/or authentication change hold time on the interface to which you are connected.

Usage Guidelines Enter `no ip ospf md5-authentication key-id` to disable this configuration.

Examples The following command sets authentication only on the OSPF 40-gigabit Ethernet 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 virtual Ethernet (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 None

Defaults Enabled

Command Modes Interface subtype configuration mode

Description Use this command to enable or disable MTU-match checking. 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.

Usage Guidelines Enter **no ip ospf mtu-ignore** to disable MTU-match checking on a specific interface.

Examples To disable MTU-match checking on a specific OSPF 40-gigabit Ethernet 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 virtual Ethernet (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} no ip ospf network	
Operands	broadcast	Network type is broadcast, such as Ethernet.
	point-to-point	Network type is point-to-point.
Defaults	None	
Command Modes	Interface subtype configuration mode	
Description	Use this command to set the network type for the interface. Point-to-point can support unnumbered links, which requires less processing by OSPF.	
Usage Guidelines	Enter no ip ospf network to remove the network-type configuration.	
NOTE The network type <i>non-broadcast</i> is not supported at this time.		
Examples	To configure an OSPF point-to-point link on the OSPF 10-gigabit Ethernet 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 virtual Ethernet (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 None

Defaults All OSPF interfaces are active.

Command Modes Interface subtype configuration mode

Description Use this command to set an OPSF interface 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 Enter **no ip ospf passive** to set an interface back to active.

Examples To set a specific OSPF 10-gigabit Ethernet 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 virtual Ethernet (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. Valid values range from 0 through 255.

Defaults The default value is 1.

Command Modes Interface subtype configuration mode

Description Use this command to set priority for DR election and backup-router election on the interface you are connected to. 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 Enter **no ip ospf priority** to use the default value.

Examples To set a priority of 10 for the OSPF router that is connected to an OSPF 10-gigabit Ethernet 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 for the OSPF router that is connected to an OSPF virtual Ethernet (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. Valid values range from 0 through 3600 seconds.

Defaults 5 seconds.

Command Modes Interface subtype configuration mode

Description Use this command to set the time between Link-State Advertisement (LSA) retransmissions to adjacent routers for this interface.

Usage Guidelines Enter **no ip ospf retransmit-interval** to reset the retransmit interval to its default.

Examples To set the retransmit interval to 10 for all OSPF routers on the OS-gigabit Ethernet 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 virtual Ethernet (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. Valid values range from 0 through 3600 seconds.

Defaults 1 second.

Command Modes Interface subtype configuration mode

Description Use this command to set the estimated time required for OSPF to send link-state update packets on the interface to which you are connected.

Usage Guidelines Enter **no ip ospf transmit-delay** to use the default value.

Examples To set a transmit delay of 10 seconds for routers on the OSPF 10-gigabit Ethernet 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 virtual Ethernet (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 pim dr-priority

Configures the designated router (DR) priority of a PIM router.

Synopsis **ip pim dr-priority** *priority-value*
 no ip pim dr-priority

Operands *priority-value* The DR priority value. Valid values range from 0 through 65535.

Defaults DR priority value is 1.

Command Modes Interface configuration mode
 Router interface configuration mode

Description Use this command to set the DR priority value of a Protocol Independent Multicast-enabled interface.

Usage Guidelines Enter **no ip pim dr-priority** to disable this feature.

Examples Setting the priority to 100.
 switch(conf-if-ext-0/15) # **ip pim dr-priority 100**

See Also **router pim**

ip pim-sparse

Enables or disables Protocol Independent Multicast Sparse Mode on a physical or a VE interface.

Synopsis **ip pim-sparse**
 no ip pim-sparse

Operands None

Defaults Protocol Independent Multicast (PIM) is not enabled on an interface.

Command Modes Interface configuration mode
 Router interface configuration mode

Description Use this command to enable or disable Protocol Independent Multicast Sparse Mode on a physical or a VE interface.

Usage Guidelines Enter **no ip pim-sparse** to disable this feature.

Examples Enabling sparse PIM on an interface
 switch(config-if-ext-0/15) # **ip pim-sparse**

See Also router pim

ip policy route-map

Enables policy-based routing (PBR) on any Layer 3 interface after ACLs and route map entries are configured.

Synopsis **ip policy route-map** *map-tag*
no ip policy route-map *map-tag*

Operands *map-tag* The name of the route-map when it was created.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to enable policy-based routing (PBR) on any Layer 3 interface after ACLs and route map entries are configured.

Usage Guidelines Enter **no ip policy route-map** to disable this feature.

Examples None

See Also **show route-map, show route-map interface**

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 Use this command to configure the IP prefix-list instance.

Usage Guidelines Enter **no ip prefix-list** 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 disabled.

Command Modes Interface subtype configuration mode

Description Use this command to enable proxy ARP on a specific interface. Proxy ARP allows a 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 Enter **no ip proxy-arp** to disable proxy ARP on a specific interface.

Examples To enable proxy ARP on a specific 10-gigabit Ethernet 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 40-gigabit Ethernet 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 <i>A.B.C.D/L A.B.C.D</i> [<i>metric</i>] [distance <i>distance</i>] [tag <i>tag</i>]	
	ip route <i>A.B.C.D/L</i> { fortygigabitethernet <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i> port-channel <i>number</i> tengigabitethernet <i>rbridge-id/slot/port</i> ve <i>vlan#</i> } [<i>metric</i>] [distance <i>distance</i>] [tag <i>tag</i>]	
	ip route <i>A.B.C.D/L null</i> <i>rbridge-id/slot/port</i> [<i>metric</i>] [distance <i>distance</i>] [tag <i>tag</i>]	
	no ip route <i>A.B.C.D/L A.B.C.D</i>	
	no ip route <i>A.B.C.D/L</i> { fortygigabitethernet <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i> port-channel <i>number</i> tengigabitethernet <i>rbridge-id/slot/port</i> ve <i>vlan_id</i> }	
	no ip route <i>A.B.C.D/L null</i> <i>rbridge-id/slot/port</i>	
Operands	<i>A.B.C.D/L</i>	Specifies the destination IP address.
	<i>A.B.C.D</i>	Specifies the IP address of the next hop.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet outgoing interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet outgoing interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet outgoing interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	ve <i>vlan_id</i>	Specifies the VLAN number. (Refer to the Usage Guidelines.)
	null <i>rbridge-id/slot/port</i>	Drops packets with this destination.
	<i>rbridge-id</i>	Specifies the RBridge ID.

2 ip route

<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
<i>metric</i>	Cost metric of the route. Valid values range from 1through 16. The default is 1.
distance <i>distance</i>	Specifies the administrative distance of the route. When comparing otherwise equal routes to a destination, a Brocade device prefers lower administrative distances over higher ones. Valid values range from 1 through 255. The default is 1.
tag <i>tag</i>	Tag value of the route to use for route filtering with a route map. Valid values range from 0through 4294967295.

Defaults Refer to the Operands descriptions for specific defaults.

Command Modes RBridge ID configuration mode

Description Use this command to add a route to the IP routing tables.

Usage Guidelines Enter **no ip route** followed by the route identifier to remove a static route.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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
```

See Also None

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.

Defaults Disabled

Command Modes RBridge ID configuration mode

Description Use this command to enable a Brocade device to use routes learned from a specified protocol to resolve a configured static route.

Usage Guidelines Enter **no ip route next-hop ospf** 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
```

See Also **ip route next-hop-enable-default, ip route next-hop-recursion, ip route next-hop-vrf**

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.

Defaults Disabled

Command Modes RBridge ID configuration mode

Description Use this command to enable a 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 Enter **no ip route next-hop-enable-default** 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
```

See Also **ip route next-hop-recursion, ip route next-hop ospf, ip route next-hop-vrf**

ip route next-hop-recursion

Enables Brocade switches 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. Valid values range from 0 through 10. The default is 3.

Defaults Next-hop recursion level is 3.

Command Modes RBridge ID configuration mode

Description Use this command to enable 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 Enter **no ip route next-hop-recursion** 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
```

See Also **ip route next-hop ospf, ip route next-hop-enable-default, ip route next-hop-vrf**

ip route next-hop-vrf

Enables the leaking of static routes from one VRF instance to another.

Synopsis **ip route** *ip_addr/mask* **next-hop-vrf vrf** *VRF_name* *next_hop_ip_addr*
no route *ip_addr/mask* **next-hop-vrf vrf** *VRF_name* *next_hop_ip_addr*

Operands *ip_addr/mask* IPv4 address in dotted-decimal notation with a CIDR notation mask.
vrf *VRF_name* Specifies the name of the target VRF instance to which route leaking is enabled.
ip_addr Next-hop IP address in the target VRF instance.

Defaults Disabled

Command Modes RBridge ID configuration mode and VRF address-family IPv4 submode

Description Use this command to enable the leaking of static routes from one VRF instance to another.

Usage Guidelines Enter **no ip route** *ip_addr mask* **next-hop-vrf** to disable the leaking of static routes.

Examples To enable static route leaking from the default VRF to VRF “brown”:

```
switch# config
switch (config)# rbridge-id 2
switch (config-rbridge-id-2)# ip route 1.1.1.0/24 next-hop-vrf brown 10.1.1.10
```

This example shows the static route leaking enabled from the default VRF to VRF “brown”:

```
switch# show running rbridge
rbridge-id 2
ip route 0.0.0.0/0 10.24.64.1
ip route 1.1.1.0/24 next-hop-vrf brown 10.1.1.10
```

See Also **ip route next-hop ospf**, **ip route next-hop-enable-default**, **ip route next-hop-recursion**, **show ip route**

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.

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command to set a router ID (the 32-bit number that uniquely identifies the device). By default, the router ID is the numerically lowest IP interface configured on the device, but you can explicitly set the router ID to any valid IP address that is not in use on another device in the network.

Usage Guidelines Enter **no ip router-id** *A.B.C.D* 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
```

See Also None

ip unreachable

Prohibits routers from forwarding an Internet Control Message Protocol (ICMP) Destination Unreachable Code 3 (port unreachable) message on a point-to-point link back onto the ingress port.

Synopsis **ip unreachable**
 no ip unreachable

Operands None

Defaults This command is enabled by default.

Command Modes Global configuration mode

Description This command prohibits routers from forwarding a Destination Unreachable Code 3 (port unreachable) message on point-to-point links back onto the ingress port.

By default, ICMP Destination Unreachable Code 3 messages are sent for a discarded IP packet. You can disable the sending of these messages.

Usage Guidelines Use the **no ip unreachable** command to disable the sending of these messages.

This is an interface-specific configuration. The configuration is persistent across a switch reload.

Examples None

See Also ipv6 unreachable

ipv6 echo-reply

Enables the generation of an Internet Control Message Protocol version 6 (ICMPv6) Echo Reply message.

Synopsis **ipv6 echo-reply**
 no ipv6 echo-reply

Operands None

Defaults None

Command Modes Global configuration mode

Description Use this command to enable the generation of an ICMPv6 Echo Reply message.

Usage Guidelines This is an interface-specific configuration. The configuration is persistent across a switch reload.

Examples None

See Also None

ipv6 icmp rate-limit

Limits the rate at which Internet Control Message Protocol (ICMP) messages are sent on an IPv6 network.

Synopsis **ipv6 icmp rate-limit** *milliseconds*
no ipv6 icmp rate-limit

Operands *milliseconds* Number of milliseconds between packets. The range is from 1 through 4294967295.

Defaults The default value is 1000 milliseconds.

Command Modes Interface configuration mode

Description This command limits the rate at which ICMP messages are sent on an IPv6 network. To protect against TCP SYN attacks, you can configure the Brocade device to drop TCP SYN packets when excessive numbers of messages are encountered. You can set threshold values for TCP SYN packets that are targeted at the router itself or passing through an interface, and drop them when the thresholds are exceeded.

Usage Guidelines The configuration is persistent across switch reload. Once it is enabled, all outbound ICMP message types are rate limited.

Examples None

See Also **ip icmp rate-limit**

ipv6 ra-guard

Protects against malicious Router Advertisements (RAs).

Synopsis **ipv6 ra-guard**
no ipv6 ra-guard

Operands None

Defaults None

Command Modes Interface configuration mode

Description Use this command to protect against malicious Router Advertisements (RAs).

When operating IPv6 in a shared Layer 2 (L2) network segment without complete SEcure Neighbor Discovery (SEND) support by all devices connected or without the availability of the infrastructure necessary to support SEND, there is always the risk of facing operational problems due to rogue RAs.

RA-Guard protects the system against generated maliciously or unintentionally by unauthorized or improperly configured routers connecting to the segment.

RA-Guard applies to an environment where all messages between IPv6 end-devices traverse the controlled Layer 2 networking devices.

Usage Guidelines Enter **no ipv6 ra-guard** to disable this feature.

Examples `switch(conf-if-te-12/2/1)# ipv6 ra-guard`

See Also **interface management**

ipv6 route

Configures a static IPv6 route.

Synopsis **ipv6 route** *IPv6_address/prefix*
 no ipv6 route *IPv6_address/prefix*

Operands *IPv6_address/prefix* Sets the IPv6 address and prefix for the next hop.
 next-hop The next-hop IPv6 address.

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command to configure a static IPv6 route.

Usage Guidelines Enter **no ipv6 route** *IPv6_address/prefix* to remove the configuration.

Examples To configure a static IPv6 route.
 switch(config-rbridge-id-2)# **ipv6 route fe80::21b:edff:fe0b:3c00/64**

See Also interface management

ipv6 unreachable

Prohibits routers from forwarding an Internet Control Message Protocol version 6 (ICMPv6) Destination Unreachable Code 3 (port unreachable) message on a point-to-point link back onto the ingress port.

Synopsis **ipv6 unreachable**
 no ipv6 unreachable

Operands None

Defaults This command is enabled by default.

Command Modes Global configuration mode

Description This command prohibits routers from forwarding an ICMPv6 Destination Unreachable Code 3 (port unreachable) message on point-to-point links back onto the ingress port.

By default, ICMPv6 Destination Unreachable Code 3 messages are sent for a discarded IP packet. You can disable the sending of these messages.

Usage Guidelines Use the **no ipv6 unreachable** command to disable the sending of these messages.

This is an interface-specific configuration. The configuration is persistent across a switch reload.

Examples None

See Also **ip unreachable**

iscsi-priority

Sets the iSCSI priority bitmap.

Synopsis **iscsi-priority** *value*
 no iscsi-priority

Operands *value* The priority bitmap value. Valid values range from 0 through 7.

Defaults Priority bitmap value is 4.

Command Modes Protocol LLDP configuration mode

Description Use this command to set the iSCSI priority bitmap for use in the DCBX iSCSI TLV.

Usage Guidelines Enter **no iscsi-priority** to return to the default value.

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 **no isl-r_rdy** or VC_RDY flow control mode.

Command Modes Interface Fibre Channel configuration mode

Description Use this command to enable inter switch 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.

Usage Guidelines Brocade recommends 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.

Enter **no isl-r_rdy** to disable ISL R_RDY mode on a port, and instead establish VC_RDY flow control.

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 Use this command to enable the keep-alive timeout.

Usage Guidelines You must be in the feature configuration mode for FCoE fabric-map for this command to function.
Enter **no keep-alive timeout** to disable the keep-alive timeout.

Examples None

See Also **fabric-map, fcoe**

I2traceroute

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

Synopsis	I2traceroute
Operands	None
Defaults	None
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 I2traceroute 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 I2traceroute command. Configuration results depend on the configuration parameters specified. The following fields display when you enter the I2traceroute 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 switches, 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • Edge rbridge-id—Enter the edge RBridge ID on which the I2traceroute 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 parameters branch as follows:

- **Protocol Type [IP]**—Enter the protocol type. You must select the IP including.
 - 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 including:
 - **TCP** (Transmission Control Protocol) is a connection-oriented protocol, which means that it requires handshaking to set up end-to-end communications.
 - **UDP** (User Datagram Protocol) 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.
- The source port number. The valid port range is 0 through 65535. This is an optional field.
- The destination port number. The valid port range is 0 through 65535. This is an optional field.

Examples This example shows 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 default-up

Activates an LACP link in the absence of PDUs.

Synopsis **lACP default-up**
 no lACP default-up

Operands None

Defaults None

Command Modes Interface configuration mode

Description Use this command to force the port to activate an LACP link if there are no PDUs available on the interface port. This command is supported on all physical interfaces.

Usage Guidelines This command is visible only if the interface is a dynamic and standard member of a port-channel.
 This command is not supported on Static LAGs.
 This command is not supported on static or dynamic Brocade Trunks.
 This command is not supported on any other types of interfaces, such as port-channel or VLAN.
 Enter **no lACP default-up** to disable this feature.

Examples switch# (conf-if-te-1/0/9)# **lACP default-up**

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. Valid values range from 1 through 65535. A lower number takes priority over a higher number.

Defaults The default value is 32768.

Command Modes Interface subtype configuration mode

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 Enter **no lacp port-priority** to return to the default value.

Examples To set the LACP port priority to 1000 for a specific 10-gigabit Ethernet 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. Valid values range from 1 through 65535.

Defaults The default 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.

Usage Guidelines Lower numerical values have higher priorities.
Enter **no lACP system-priority** to reset the system priority to the default value.

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 the Link Aggregation Control Protocol (LACP) to exchange packets on an interface before invalidating a received data unit (DU).

Synopsis **lacp timeout {long | short}**
no lacp timeout

Operands

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.
For standard LAGs, the default value is the **long** timeout.

Command Modes Interface subtype configuration mode

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 Enter **no lacp timeout** to return to the default values.

Examples To use the LACP long-timeout value on a specific 10-gigabit Ethernet 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*] [**domain** *basedn*] [**timeout** *secs*] [**retries** *num*]
no ldap-server host {*ipaddr* | *FQDN*}

Operands *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 the TCP port used to connect the AD server for authentication. The port range is from 1024 through 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 through 60 seconds.

retries *num* Specifies the number of retries for the server connection. The range is 0 through 100.

Defaults • **Timeout:** 5 seconds
 • **Port:** 389
 • **Retries:** 5

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. A maximum of 5 LDAP servers can be configured on a switch. Executing “no” on an attribute sets it with its default value.

Usage Guidelines Enter **no ldap-server host** to delete the server configuration.

 Enter **no ldap-server host** with a parameter to restore the default value for that parameter.

 Invoking **no** on an attribute sets the attribute with its 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 domain 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
```

2 ldap-server host

Executing **no** on an attribute sets it with its default value.

```
switch(config)# no ldap-server host 10.24.65.6 retries
```

Attributes holding default values will not be displayed.

```
switch# show running-config ldap-server host 10.24.65.6  
ldap-server host 10.24.65.6  
port      3890  
domain    security.brocade.com
```

See Also **certutil import ldapca, ldap-server maprole, show running-config ldap-server**

Idap-server maprole

Maps an Active Directory (AD) group to a switch role.

Synopsis **Idap-server maprole group** *group_name* **role** *role_name*
no Idap-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 Enter **no Idap-server maprole group** *group_name* without the **role** *role_name* parameter 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)# **Idap-server maprole group Administrator role admin**

To remove the mapping:

switch(config)# **no Idap-server maprole group Administrator**

See Also certutil import ldapca, Idap-server host, show running-config Idap-server

license add

Adds a license key to a switch.

Synopsis	license add { licstr <i>licenseString</i> FTP-URL <i>ftpPath</i> SCP-URL <i>scpPath</i> } [rbridge-id <i>rbridge-id</i>]	
Operands	licstr <i>licenseString</i>	Specifies the license string to be added to the switch. The license string must be enclosed in double quotation marks. A maximum of 256 characters is allowed.
	FTP-URL <i>ftpPath</i>	Specifies a URL from which to transfer license information using FTP. <i>ftp://username:password@hostname/ filepath</i>
	SCP-URL <i>scpPath</i>	Specifies a URL from which to transfer license information using SCP. <i>scp://username:password@hostname/ filepath</i>
	rbridge-id <i>rbridge-id</i>	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 may need to disable and re-enable the affected 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: <pre>switch# license add licstr "*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvv13Strvw1:fUjANF av5W:gWx3hH2:9RsMv3BHfeCRFM2gJ9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#" Adding license [*B r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvv13Strvw1:fUjANF av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9NlkrdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#]</pre> To add a Dynamic Ports on Demand (DPOD) license on a switch that does not support the feature: <pre>switch# license add licstr "*B a6q3zwcUaNkWHPOfVf8afFZqHYype6sQxaEr5HIeFD3nba74i43BnRt6T8b2sDPtVMKuMfUPwV8NvHDX xFgbB3f2w3pJNlujxLVdIVkXdoNHf6i4SzwuvimIj0ORN:JOojLU#" License Added [*B a6q3zwcUaNkWHPOfVf8afFZqHYype6sQxaEr5HIeFD3nba74i43BnRt6T8b2sDPtVMKuMfUPwV8NvHDX xFgbB3f2w3pJNlujxLVdIVkXdoNHf6i4SzwuvimIj0ORN:JOojLU#]</pre> <pre>switch# show license xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx Ports on Demand license - not applicable on this platform license Feature name:PORTS_ON_DEMAND_1</pre>	
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

<code>licstr licenseString</code>	Removes the specified license string and associated feature. The license string must be enclosed in double quotation marks.
<code>licstr feature</code>	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, LAYER_3, PORT_10G_UPGRADE and PORT_OG_UPGRADE.
<code>rbridge-id ID</code>	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 first clear all license-related configurations, and possibly disable and re-enable 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. To remove the 10G and 40G Port Upgrade licenses, you must remove all non-Base-allowance port reservations for the respective license type.

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
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvv13Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9N1krdIiBPBOa4xfSD2jf,Xx1RwksliX8fH6gpx7,73t#
```

```
Removing license for rbridge-id 2 [*B
r84pNRtHKdRZujmwAUT63GORXIpBhBZK0ckRq6Bvv13Strvw1:fUjANF
av5W:gWx3hH2:9RsMv3BHfeCRFM2gSLj9N1krdIiBPBOa4xfSD2jf,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 range from 0 through 136.

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.

The **line vty exec timeout** 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 **line vty exec timeout** 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.

Enter **no line vty exec-timeout** to disable auto-logout and delete the timeout value.

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 a line card (interface module).

Synopsis **linecard** *slot_number linecard_type*
 no linecard *slot_number*

Operands *slot_number* Specifies the slot number to be configured. Line card slots are slots 1 through 4 on a Brocade VDX 8770-4 and slots 1 through 8 on a Brocade VDX 8770-8.

linecard_type Specifies the type of line card. Enter **linecard slot_number linecard_type ?** to display currently supported types.

Defaults None

Command Modes Global configuration mode
 RBridge ID configuration mode

Description Use this command to configure the specified slot for an line card of a given type.

The command is executed in the context of the given RBridge. You must first enter the rbridge-id context for the specific line card. Once you are in the rbridge-id context, enter **linecard slot_number linecard_type** to configure the slot.

Usage Guidelines If you replace a given line card with another one of a different type, you must remove the configuration and then reconfigure the slot.

The line card must be powered off before you can remove the slot configuration.

The LC72x1G type displayed under “possible completion” is not supported.



CAUTION

Enter **no linecard** to remove the slot configuration. **When hot-swapping line cards of different types, copy the running-config file to the startup-config file before rebooting. This ensures that the desired changes are persistent in case there are any hardware or software incompatibilities.**

Examples To configure a slot for an line card 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
```

2 linecard

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 setting is **auto**.

Command Modes Interface subtype configuration mode

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 Enter **no lldp dcbx-version** to return to the default setting.

Examples To specify that the CEE version be used on a specific 10-gigabit Ethernet 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 LLDP is enabled at both the global and interface levels.

Command Modes Interface subtype configuration mode

Description Use this command to disable LLDP on the interface.

Usage Guidelines Enter **no lldp disable** to enable LLDP on a specific interface.

Examples To disable LLDP on a specific 10-gigabit Ethernet interface:

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

To enable LLDP on a specific 40-gigabit Ethernet 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

Sets 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. Valid values range from 0 through 7.

Defaults Priority value is 4.

Command Modes Interface subtype configuration mode

Description Use this command to specify the priority that will be advertised in the DCBX iSCSI TLV. 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 Enter **no lldp iscsi-priority** to return to the default setting.

Examples To set the iSCSI priority value to 5 on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9  
switch(conf-if-te-178/0/9)# lldp iscsi-priority 5
```

See Also **interface**, **lldp dcbb-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. Valid profile name length is between 1 and 32 characters.

Defaults LLDP profile name.

Command Modes Interface subtype configuration mode

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.

Enter **no lldp profile** to delete the profile from the interface.

Examples To apply an LLDP profile called *test* on an specific 10-gigabit Ethernet 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**

load-balance

Set load balancing.

Synopsis **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**]

no load-balance

Operands	dst-mac-vid	Specifies that destination MAC address and VID-based load balancing will be used.
	src-dst-ip	Specifies that source and destination IP address-based load balancing will be used.
	src-dst-ip-mac-vid	Specifies that source and destination IP and MAC address and VID-based load balancing will be used.
	src-dst-ip-mac-vid-port	Specifies that source and destination IP, MAC address, VID and TCP/UDP port-based load balancing will be used. This is the default.
	src-dst-ip-port	Specifies that source and destination IP and TCP/UDP port-based load balancing will be used.
	src-dst-mac-vid	Specifies that source and destination MAC address and VID-based load balancing will be used.
	src-mac-vid	Specifies that source MAC address and VID-based load balancing will be used.

Defaults The default setting is the operand *src-dst-ip-mac-vid-port*, which means that source and destination IP, MAC address, VID and TCP/UDP port-based load balancing are used.

Command Modes Port-channel configuration mode

Description Use this command to configure desired load balancing settings.

Usage Guidelines Use the **no** form of this command to return to the default setting.

Examples To set load balancing to use the destination MAC address and VID-based load balancing:

```
switch# configure
switch(config)# interface port-channel 10
switch(config-Port-channel-10)# load balance dst-mac-vid
```

See Also None

local-as (BGP)

Specifies the autonomous system number (ASN) where the device resides.

Synopsis **local-as** *num*
 no local-as

Operands *num* The local ASN. The range is from 1 through 4294967295.

Defaults None

Command Modes BGP configuration mode

Description Use this command to enable specify an ASN for a given device to associate it with other devices in its autonomous system.

Usage Guidelines ASNs in the range from 64512 through 65535 are private numbers that are not advertised to the external community.

Use the **no** form of this command to remove the ASN from the device.

Examples `switch(config)# rbridge-id 10`
 `switch(config-rbridge-id-10)# router bgp`
 `switch(config-bgp-router)# local-as 777`

See Also None

log-dampening-debug (BGP)

Logs dampening debug messages.

Synopsis **log-dampening-debug**
 no log-dampening-debug

Operands None

Defaults This option is disabled.

Command Modes BGP configuration mode

Description Use this command to log dampening debug messages.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **log-dampening-debug**

See Also None

logging auditlog class

Sets the severity levels for the audit log class.

Synopsis **logging auditlog class** *class*

no logging auditlog class *class*

Operands*class* Specifies the class name of the audit log. Valid classes are CONFIGURATION, FIRMWARE, and SECURITY.

Defaults CONFIGURATION, FIRMWARE, and SECURITY audit log classes are enabled.

Command Modes Global configuration mode

Description Use this command to set the class for the audit log.

Usage Guidelines This command is supported only on the local switch.
 This command is not supported on the standby management module.
 The total message storage available is 2048 messages.
 Enter **no logging auditlog class** *class* to remove the audit logging for the specified class.

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 and allows users to temporarily stop showing RASLog messages on the console.

Synopsis **logging raslog console severity**
 no logging raslog console severity
 logging raslog console stop [*minutes*]

logging raslog console start *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.

Operands

start Initiates RASLog messages.

stop Stops RASLog messages.

Defaults Severity level is INFO.

Command Modes Global configuration mode

Description Use this command to set the severity levels for the RASLog console.

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

 This command is not supported on the standby management module.

 The total message storage available is 2048 messages.

 When stopping or starting RASLog messages, the commands are not persistent and therefore are not configuration commands.

 If the command **logging raslog console stop** *minutes* is invoked before the previous time value expires, the latest CLI duration applies.

Examples Standalone

To set the RASLog severity level:

```
switch(config)# logging raslog console WARNING
```

To reset the RASLog severity levels to the default value.

```
switch(config)# no logging raslog console
```

To stop RASLog messages for 1 minute:

```
switch# logging raslog console stop 1
Logging message have been blocked on console for 1 minutes
```

To start RASLog messages:

```
switch# logging raslog console start
2013/11/14-08:42:57, [RAS-3008], 5348, M2 | Active, INFO, VDX8770-4, Logging
messages to console has been reset by user.
```

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 <i>log_level</i>	
Operands	<i>log_level</i>	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	Syslog level is LOG_LOCAL7.	
Command Modes	Global configuration mode	
Description	Use this command to configure the log level for all error log entries to forward to one or more specified servers. You can configure up to four servers.	
Usage Guidelines	When used without a log level parameter, use this command to display 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: <pre>switch(config)# logging syslog-facility local LOG_LOCAL5</pre>	
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*

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 is not shown in the Brocade Network OS database.

port *value* Configures the port for the syslog server.

Defaults If the secure parameter is set to **true** and the port number is not specified, the default port number of 6514 is used.

The default value for the secure parameter 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.

The **certutil import syslogca** 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 parameter is set to **false**, you are not able to set the port number.

Enter **no logging syslog-server** to remove the specified IP address.

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
```

To remove a syslog server port:

```
switch(config)# no logging syslog-server 10.17.17.203 secure port 1999
switch(config)# do show running-config logging syslog-server
logging syslog-server 10.17.17.203
secure
```

See Also **certutil import syslogca**, **logging syslog-facility local**, **show running-config logging syslog-facility**, **show running-config logging syslog-server**

logical-chassis principal-priority

Sets the priority of a switch to assign a specific RBridge ID the role of principal node in a logical chassis cluster.

Synopsis **logical-chassis principal-priority** *priority-value*
no logical-chassis principal-priority

Operands *priority-value*

Sets the priority for the switch. A lower number means a higher priority. Values range from 1 through 128.

Defaults None

Command Modes RBridge ID configuration mode

Description If all switches boot up at the same time, the default priority is the same and all switches will compare their mutual intents. The switch with the lowest switch WWN becomes the principal switch. However, you can use this command to select the principal switch in a logical chassis cluster. For this command to take effect, you need to issue the **logical-chassis principal-switchover** command.

Usage Guidelines This command can be used only on nodes that are part of a logical chassis cluster. The node, however, can be disconnected from the cluster when you issue the command.

Use the **no** form of this command to remove a priority value from this node.

You can view the principal priority in both the **show running config** (using the **rbridge-id** operand) and **show vcs detail** command outputs (both are run in Privileged EXEC mode).

Examples To set the principal priority to 5 for switch that is in logical chassis cluster:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# logical-chassis principal-priority 5
```

See Also **logical-chassis principal-switchover**

logical-chassis principal-switchover

Triggers a fabric reformation and elects a principal node based on the principal priority value.

Synopsis	logical-chassis principal-switchover
Operands	None
Defaults	None
Command Modes	Privileged EXEC mode
Description	Issue this command after you have used the logical-chassis principal-priority <i>priority-value</i> command so that the priority you set takes effect and a new principal node is selected on the cluster.
Usage Guidelines	None
Examples	<pre>switch# configure switch(config)# rbridge-id 5 switch(config-rbridge-id-5)# logical-chassis principal-priority 1 switch(config-rbridge-id-5)# end switch# logical-chassis principal-switchover</pre>
See Also	logical-chassis principal-priority

long-distance

Configures a Fibre Channel port to support long distance.

Synopsis `long-distance {IO | le | ld | ls}`

Operands

IO	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 1452 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), 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 1452 full-size frame buffers are reserved for data traffic, depending on the specified desired distance (desire-distance).

Defaults The value is **IO**.

Command Modes Fibre Channel interface configuration 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 30 km.

Synopsis `long-distance-isl {2000 | 5000 | 10000 | 30000}`
`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.
30000	Specifies a 30 km distant link. DCB/FCoE capabilities are not supported with this setting.

Defaults The default is 2 km.

Command Modes Interface subtype configuration mode

Description Use this command to extend an ISL link up to 30 km. An ISL port with PFC supports up to 10 km distance on Brocade VDX 6710, 6720, and 6730 series platforms. Up to 10 km links are lossless. You can have eight 1 km 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 Metro VCS supports long-distance ISL ports up to 30 km on the Brocade VDX platforms listed below. Links up to 10 km are lossless. You can have eight 1-km 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.

Limitations for long-distance Metro VCS

Supported hardware	Extended ISL up to 2 km	Extended ISL up to 5 km	Extended ISL up to 10 km	Extended ISL up to 30 km
Brocade VDX 6720-60	yes	yes	yes	yes
Brocade VDX 6730-76	yes	yes	yes	yes
Brocade VDX 6740	yes	yes	yes	yes
Brocade VDX 8770 - VDX LC48x10G line card	yes	yes	yes	yes

The following displays the limitations on extended ISL for Network OS hardware.

Conditions for long distance Metro VCS

Condition	Extended ISL up to 2 km	Extended ISL up to 5 km	Extended ISL up to 10 km	Extended ISL up to 30 km
Support for lossless FCoE/iSCSI traffic on the Metro VCS port-group	yes	yes	yes	no
Layer 2/IP Lossy Traffic support	yes	yes	yes	yes
Number of Metro VCS long distance ports supported per port group	1	1	1	1

Conditions for long distance Metro VCS (Continued)

Condition	Extended ISL up to 2 km	Extended ISL up to 5 km	Extended ISL up to 10 km	Extended ISL up to 30 km
Number of regular ISLs supported on a port group configured for long distance	1	1	0	0
Trunking support between multiple LD ISLs	no	no	no	no
CEE map or FCoE port allowed in same port-group	no	no	no	no
eNS Sync (MAC address table sync)	yes	yes	yes	yes
Zoning	yes	yes	yes	yes
HA failover	yes	yes	yes	yes
Node redundancy check	yes	yes	yes	yes
vMotion	yes	yes	yes	yes
Maximum PFCs Supported	3 (2 on the Brocade VDX 6740)	3 (2 on the Brocade VDX 6740)	3 (2 on the Brocade VDX 6740)	3 (2 on the Brocade VDX 6740)

The following displays the port groups and number of port groups available on each platform for long distance Metro VCS.

Long distance Metro VCS port-group schema

Platform	Port groups	Number of port groups on platform
Brocade VDX 6720-60 (10Gbe)	1-10, 11-20, 21-30, 31-40, 41-50, 51-60	6
Brocade VDX 6730-76 (10Gbe)	1-10, 11-20, 21-30, 31-40, 41-50, 51-60	6
Brocade VDX 6740	1-32, 33-48	2*
Brocade VDX 8770 (VDX LC48x10G linecard)	1-8, 9-16, 17-24, 25-32, 33-40, 41-48	6 per 10G blade

*Not a valid deployment scenario at distances longer than 5 km, as no normal ISLs are allowed if both port-groups are configured with long-distance ISLs for 10 km and 30 km. 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.

Enter **no long-distance-isl** to revert to the default value.

Examples To extend the support of an ISL port with PFC by a distance of 5 km on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# long-distance-isl 5000
```

See Also interface, isl-rdy, long-distance

mac

Allows the user to add a MAC address to a MAC address group in a service or transport VF configuration supporting multitenancy in a Virtual Fabrics context.

Synopsis **mac** *mac_address*
 no mac *mac_address*

Operands *mac_address* Specifies a MAC address in dot-separated hexadecimal notation.

Defaults None

Command Modes MAC group configuration mode

Description Use this command in MAC group configuration mode to add a MAC address to a MAC address group in a service or transport VF configuration supporting multitenancy in a Virtual Fabrics context.

Usage Guidelines Enter MAC group configuration mode by using the **mac group** *mac-group-id* global configuration command.

Enter **no mac** *mac_address* to remove a MAC addresses from the group.

NOTE

You can add or remove only one MAC address per line.

Examples To enter MAC group configuration mode and add a MAC address to the group:

```
switch(config)# mac-group 1  
switch(config-mac-group 1)# mac abc1.abc2.abc3
```

To remove a MAC address from the group:

```
switch(config-mac-group 1)# no mac abc1.abc2.abc3
```

See Also mac-group, vcs virtual-fabric enable

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 No access lists are applied to the interface.

Command Modes Interface subtype configuration mode

Description Use this command to apply a MAC ACL to a supported interface.
 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.
 Enter **no mac access-group** *name* {**in** | **out**} 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 10-gigabit Ethernet 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 name must start with a letter ('a' to 'z', 'A' to 'Z'), or a number ('1' to '9'), and the only special characters allowed are underscores and hyphens. The name must be between 1 and 63 characters in length.

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.

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.
 Enter **no mac access-list extended** to remove the access list.

Examples To create a MAC extended ACL named mac1:

```
switch(config)# mac access-list extended mac1
switch(config-macl-ext)#
```

To delete a MAC extended ACL named mac1:

```
switch(config-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 name must start with a letter ('a' to 'z', 'A' to 'Z'), or a number ('1' to '9'), and the only special characters allowed are underscores and hyphens. The name must be between 1 and 63 characters in length.

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.
 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.
 Enter **no mac access-list standard** to remove the access list.

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 configuration mode

Description Use this command to enable or disable the MAC address reduction feature.

Usage Guidelines None

Examples None

See Also None

mac-address-table

Sets the aging time or add static addresses to the MAC address table.

Synopsis **mac-address-table** {**aging-time** *seconds* | **static** *mac-addr* **forward** [**port-channel** *number*] | **tengigabitethernet** *rbridge-id/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, valid values range from 10 through 100000. For Brocade VCS Fabric mode, valid values range 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. Valid values range from 1 through 63.

tengigabitethernet *rbridge-id/slot/port* Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This 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-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. 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 the Usage Guidelines.

Defaults 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).
 On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

2 mac-address-table

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Enter **no mac-address-table** to reset the values to their defaults.

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-group

Allows the user to create a MAC address group into which one or more end-station MAC addresses are defined, supporting service or transport VFs in a Virtual Fabrics context.

Synopsis **mac-group** *mac-group-id*
no mac-group *mac-group-id*

Operands *mac-group-id* A fabric-wide ID. Values range from 1 through 500.

Defaults None

Command Modes Global configuration mode

Description Use this command to create a MAC address group into which one or more end-station MAC addresses are defined, supporting service or transport VFs in a Virtual Fabrics context. The group is used in MAC-based VLAN classification at the access port.

Usage Guidelines Use this command to enter MAC group configuration mode. In that mode, use the **mac** command to enter one or more MAC addresses that become members of the group.

Enter **no mac-group** *mac-group-id* to delete the group and all MAC addresses associated with it.

NOTE

You can add or remove only one MAC address per line.

Examples To enter MAC group configuration mode and add a MAC address to the group:

```
switch(config)# mac-group 1  
switch(config-mac-group 1)# mac abc2.abc2.abc2
```

To remove a MAC address from the MAC group:

```
switch(config-mac-group 1)# no mac abc1.abc2.abc3
```

To remove a MAC group and its associated MAC addresses:

```
switch(config)# no mac-group 1
```

See Also mac, vcs virtual-fabric enable

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. Valid values range 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 Use this command to force the rebalancing of MAC table EXM entries.

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 rebalanced 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 current node's ID are not allowed.

This command does not function in standalone mode.

Examples This example rebalances the EXM entries on RBridge 1 (for vLAG 10):

```
switch# mac-rebalance port-channel 10 rbridge-id 1
```

See Also None

management

Enables a variety of Dynamic Host Configuration Protocol (DHCP) management options.

Synopsis **management** [**interface** {**autoconfig** {**dhcp** | **dhcpv6**}]
 no management

Operands	interface	Enables management options.
	autoconfig	Enables automatic configuration of DHCP.
	dhcp	Enables DHCP for IPv4.
	dhcpv6	Enables DHCP for IPv6.

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command to configure a variety of DHCP management options.

Usage Guidelines Use the **no** version of this command to disable this feature.

Examples None

See Also None

2 map

map

Enables map configuration mode.

Synopsis **map {default}**

Operands **default** This keyword is required.

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**

map fport interface fcoe

Maps VF_Ports to N_Ports in Access Gateway (AG) mode and removes VF_Port to N_Port mapping.

Synopsis **map fport interface fcoe** *port*

Operands *port* VF_Port number

Defaults None.

Command Modes N_Port configuration mode

Description Use this command to specify a route that AG will use to direct traffic from a device (host or target) on a VF_Port to a fabric switch port connected to an Access Gateway N_Port. The process of specifying routes is called “mapping.” Default mapping is enabled for the switch when enabling AG for the first time, You can use the **map** command to change the default mapping.

Usage Guidelines You must be in the configuration mode for the specific N_Port where you want to map a VF_Port (refer to “nport”). N_Ports are designated by the format *rbridge-id/port group/N_Port*, such as 3/0/4 for RBridge 3. Use this format to correctly identify the N_Port in N_Port configuration mode. VF_Ports are identified by the format *domain/rbridge-id/VF_Port*, such as 1/2/26.

Examples Map VF_Port 1/2/26 to N_Port 2/0/4.

```
sw0(config-rbridge-id-2-ag-nport-if-fi-
2/0/4)# map fport interface fcoe 1/2/26
```

Remove map from VF_Port 1/2/26 to N_Port 2/0/4.

```
w0(config-rbridge-id-2-ag-nport-if-fi-
2/0/4)# no map fport interface fcoe 1/2/26
```

See Also **show ag map, nport**

map qos

Adds the QoS profile name as an action to the policy map.

Synopsis **map qos** *profile_name*

Operands *profile_name* Designates the name of the QoS profile to be added.

Defaults None

Command Modes Policy-map configuration mode

Description Use this command to add the QoS profile name as an action to the policy map.

Usage Guidelines None

Examples None

See Also **class, policy-map**

map sflow

Adds the sFlow profile name as an action to the policy map.

Synopsis **map sflow** *profile_name*

Operands *profile_name* Designates the name of the sFlow profile to be added.

Defaults None

Command Modes Policy-map configuration mode

Description Use this command to add the sFlow profile name as an action to the policy map.

Usage Guidelines None

Examples Typical command usage:

```
switch(config)# policy-map p1  
switch(config-policymap)# class c1  
switch(config-policyclass)# map sflow mysflowmap
```

See Also **class, policy-map**

match

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

Synopsis **match** *criteria*

Operands *criteria* Used while in config-classmap mode to configure the match criteria for the class.

Defaults The only available match criteria at this time is “match any.”

Command Modes Class-map configuration mode

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 is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples To configure “match any” match criteria for the class while in config-classmap mode:
`switch(config-classmap)# match any`

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

match (route map)

Defines a variety of match conditions for a route map.

Synopsis	match {[as-path <i>name</i>] [community <i>acl</i> exact-match] [ip address <i>acl</i> prefix-list <i>string</i>] [ip route-source <i>acl</i> prefix <i>name</i>] [metric <i>num</i>] [next-hop <i>address-filter-list</i>] [route-type [internal external-type1 external-type2]] [level-1 level-2 level-1-2] [tag <i>tag-value</i>] interface <i>interface interface interface . . . interface</i> [protocol bgp static-network protocol bgp external protocol bgp internal]] [ip address <i>acl</i> <i>acl-name</i>]}	
	no match no match { ip address <i>acl</i> <i>acl-name</i> }	
Operands	as-path	Specifies an AS-path ACL that is configured by the ip as-path access-list command.
	<i>name</i>	Name of the ACL.
	community <i>acl</i> exact-match	Matches a route if and only if the route community attributes field contains the same community numbers specified in the match statement.
	ip address	Specifies an IP ACL or prefix list.
	<i>acl</i>	ACL that is configured by the ip as-path access-list command.
	prefix-list	Specifies an IP prefix list.
	<i>string</i>	Name of the prefix list.
	ip route-source	Specifies an IP route source ACL or prefix list.
	<i>acl</i>	ACL that is configured by the ip as-path access-list command.
	prefix	IP prefix.
	<i>name</i>	Name of the prefix.
	metric	Compares the route MED (metric) to the value specified by <i>num</i> .
	<i>num</i>	BGP4 route metric.
	next-hop	Compares the IPv4 address of the route next hop to the specified IP address filters. The filters must be already configured by means of the distribute-list command.
	<i>address-filter-list</i>	Number of the address filter list configured by means of the neighbor distribute-list command.
	route-type	Compares a route type to a specified value. Applies to OSPF routes only.
	internal	Specifies an internal route.
	external-type1	Specifies an External Type 1 route.
	external-type2	Specifies an External Type 2 route.
	level-1	Compares IS-IS routes only with routes in the same area.
	level-2	Compares IS-IS routes only with routes in different areas, but within a domain.

2 match (route map)

level-1-2	Compares IS-IS routes with routes in the same and in different areas, but within a domain.
tag	Compares the route tag with the specified tag value.
<i>tag-value</i>	Tag value.
interface	Specifies an interface.
<i>interface</i>	Interface type.
protocol bgp static-network	Matches on BGP4 static network routes.
protocol bgp external	Matches on EBGp routes.
protocol bgp internal	Matches on IBGP routes.
ip address acl	Distributes any routes that have a destination network number address that is permitted by a standard or extended access list, and performs policy routing on packets.
<i>acl-name</i>	The name of the ACL in which matching criteria are specified.

Defaults This option is disabled.

Command Modes Route-map configuration mode

Description Use this command to define a variety of conditions for a route map.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To match AS-path ACL 1:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# route-map myroutes  
switch(config-route-map myroutes)# match as-path 1
```

See Also route-map, ip as-path access-list, neighbor distribute-list

match access-list

Configures the access control list to be used with the class map.

Synopsis **match access-list** *acl_name*

Operands *acl_name* Any valid MAC ACL access list name.

Defaults None

Command Modes Class-map configuration mode

Description Use this command to configure the access control list to be used with the class map for flow-based QoS.

Usage Guidelines None

Examples Example command:

```
switch(config-classmap) #match access-list engineeringACL
```

See Also **class-map**

match as-path

Matches an AS-path access list name in a route-map instance.

Synopsis **match as-path** *name*
 no match as-path

Operands *name* Name of an AS-path access list. Range is from 1 through 32 ASCII characters.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to match an AS-path access list name in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

match community

Matches a BGP community access list name in a route-map instance.

Synopsis **match community** *name*
 no match community

Operands *name* Name of a BGP community access list. Values range from 1 through 32 ASCII characters.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to match a BGP community access list name in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

match interface

Matches interface conditions in a route-map instance.

Synopsis **match interface** [**fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **loopback** | **tengigabitethernet** *rbridge-id/slot/port* | **ve** *rbridge-id/slot/port*]

 no match interface

Operands	fortygigabitethernet	Specifies a 40-GbE interface.
	gigabitethernet	Specifies a 1-GbE interface.
	loopback	Specifies a loopback port. Values range from 1 through 255.
	tengigabitethernet	Specifies a 10-GbE interface.
	ve	Specifies a virtual Ethernet port. Range is from 2 through 4090.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies the slot number.
	<i>port</i>	Specifies the port number.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to configure the interface match clause in a route-map instance. A maximum of three interfaces is supported.

Usage Guidelines None

Examples None

See Also **route-map**

match ip address

Matches IP address conditions in a route-map instance.

Synopsis **match ip address prefix-list** *name*
 no match ip address prefix-list *name*

Operands *name* Name of the prefix list. Range is from 1 through 32 ASCII characters.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to specify an IP prefix match clause in a route-map instance.

Usage Guidelines None

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

Matches IP next-hop match conditions in a route-map instance.

Synopsis **match ip next-hop prefix-list** *name*
 no match ip next-hop

Operands **prefix list** *name* Specifies a prefix list. Values range from 1 through 32 ASCII characters.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to specify an IP next-hop match clause in a route-map instance.

Usage Guidelines None

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

Matches a route metric in a route-map instance.

Synopsis **match metric** *value*
 no match metric

Operands *value* Route metric. Values range from 0 through 4294967295.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to specify a route-map metric in route-map instance.

Usage Guidelines None

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 protocol bgp

Matches BGP routes on protocol types and subtypes in a route-map instance.

Synopsis **match protocol bgp** [external | internal | static-network]
no match protocol bgp

Operands **external** Matches EBGp routes.
 internal Matches IBGP routes.
 static-network Matches BGP static routes. This is applicable only for BGP outbound policy.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to match BGP routes on protocol types and subtypes in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

match route-type

Matches a route type in a route-map instance.

Synopsis **match route-type** [internal | **type-1** | **type-2**]
 no match route-type

Operands	internal	Internal route type
	type-1	OSPF external route type 1
	type-2	OSPF external route type 2

Defaults None

Command Modes Route-map configuration mode

Description Use this command to match a route type in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

match tag

Matches a route tag in a route-map instance.

Synopsis **match tag** *value*
no match tag

Operands *value* The range of valid values is from 0 through 4294967295.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to match routes with a specified tag.

Usage Guidelines None

Examples None

See Also **route-map**

max-age

Sets the interval time in seconds between messages that the spanning tree receives from the interface.

Synopsis **max-age** *seconds*
 no max-age

Operands *seconds* Configures the Spanning Tree Protocol interface maximum age. Valid values range from 6 through 40.

Defaults 20 seconds.

Command Modes Protocol Spanning Tree configuration 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.

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

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context

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:

$$2 * (\text{forward-delay} - 1) \geq \text{max-age} \geq 2 * (\text{hello-time} + 1)$$

If xSTP is enabled over VCS, this command must be executed on all RBridges.

Enter **no max-age** to return to the default configuration.

Examples To configure the maximum-age to 10 seconds:

```
switch(conf-rstp) # max-age 10
```

See Also **forward-delay, hello-time**

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.
Valid values range from 1 through 40.

Defaults 20 hops

Command Modes Protocol Spanning Tree MSTP configuration 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.

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.

Enter **no max-hops** to return to the default value.

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-mcache

Configures the maximum multicast cache size.

Synopsis **max-mcache** *num*
 no max-mcache

Operands *num* Number of entries in the multicast cache. Valid values range from 1 through 2048.

Defaults Multicast cache size is 2048 entries.

Command Modes PIM router configuration mode

Description Use this command to set the maximum size of the multicast cache.

Usage Guidelines Enter **no max-mcache** to disable this feature.

Examples Setting the multicast cache to 500 entries.
 switch(conf-pim-router) # **max-mcache 500**

See Also **ip multicast-boundary, router pim, show ip pim mcache, show ip pim-sparse**

max-metric router-lsa (OSPF)

Advertises the maximum metric value in different Link State Advertisements (LSAs).

Synopsis `max-metric router-lsa [all-vrfs] [all-lsas | summary-lsa metric-value | external-lsa metric-value | link {ptp | stub | transit | all} | on-startup {time | wait-for-bgp} [all-lsas | summary-lsa metric-value | external-lsa metric-value | link {ptp | stub | transit | all}]]`

`no max-metric router-lsa [all-vrfs] [all-lsas | summary-lsa metric-value | external-lsa metric-value | link {ptp | stub | transit | all} | on-startup {time | wait-for-bgp} [all-lsas | summary-lsa metric-value | external-lsa metric-value | link {ptp | stub | transit | all}]]`

Operands	all-vrfs	Applies the configuration change to all instances of OSPF.
	on-startup	Applies the configuration change at the next OSPF startup.
	<i>time</i>	Sets the time (in seconds) for which the specified links in Router LSAs are advertised when the metric is set to the maximum value of 0xFFFF. The range for <i>time</i> is 5 to 86,400.
	wait-for-bgp	Indicates that OSPF should wait for either 600 seconds or until BGP has finished route table convergence, whichever happens first, before advertising the links with the normal metric.
	summary-lsa <i>metric-value</i>	Modifies the metric of all summary type 3 and type 4 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777214 (0x00001 – 0x00FFFFE), and the default is 16711680 (0x00FF0000).
	external-lsa <i>metric-value</i>	Modifies the metric of all external type 5 LSAs to equal the specified value or a default value. The range for metric value is 1 to 16777214 (0x00001 - 0x00FFFFE), and the default is 16711680 (0x00FF0000).
	all-lsas	Sets the summary-lsa and external-lsa optional parameters to the corresponding default max-metric value. For a non-default instance of OSPF, only the summary-lsa and external-lsa parameters are set.
	link	Specifies the types of links for which the maximum metric is advertised. By default, the maximum metric is advertised only for transit links.
	all	Advertises the maximum metric in Router LSAs for all supported link types.
	ptp	Advertises the maximum metric in Router LSAs for point-to-point links.
	stub	Advertises the maximum metric in Router LSAs for stub links.
	transit	Advertises the maximum metric in Router LSAs for transit links. This is the default link type.

Defaults Refer to the Operands for various defaults within the command.

Command Modes OSPF VRF router configuration mode

Description Use this command to set the maximum metric value advertised in different Link State Advertisements (LSAs). 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 Enter **no max-metric router-lsa all-lsas** to disable advertising the maximum metric value in different LSAs.

Examples To advertise the maximum metric value using the **all-lsas** option:

```
switch# configure  
switch(config)# rbridge-id 5  
switch(config-rbridge-id-5)#router ospf  
switch(config-router-ospf-vrf-default-vrf)# max-metric router-lsa all-lsas
```

See Also None

max-route

Sets the maximum number of routes for VRF.

Synopsis **max-route** *value*

Operands *value* The maximum number of routes.

Defaults None

Command Modes VRF configuration command

Description Use this command to set the maximum number of routes for VRF.

Usage Guidelines None

Examples None

See Also **vrf**

maxas-limit (BGP)

Imposes a limit on the number of autonomous systems in the AS-PATH attribute.

Synopsis **maxas-limit** {in} *num*
 no maxas-limit {in} *num*

Operands **in** Allows an AS-PATH attribute from any neighbor imposing a limit on the number of autonomous systems.
 num Valid range is from 0 through 300.

Defaults This option is disabled.

Command Modes BGP configuration mode

Description Use this command to impose a limit on the number of autonomous systems in the AS-PATH attribute.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples The following example sets the limit on the number of autonomous systems in the AS-PATH attribute to 100.

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# maxas-limit 100
```

See Also None

maximum-paths (BGP)

Changes the maximum number of BGP4 shared paths.

Synopsis	maximum-paths <i>num</i> use-load-sharing no maximum-paths	
Operands	<i>num</i>	Maximum number of paths across which the device balances traffic to a given BGP4 destination.
	use-load-sharing	Uses the maximum IP ECMP path value that is configured by means of the ip load-sharing command.
Defaults	This option is disabled.	
Command Modes	BGP address-family IPv4 unicast configuration mode	
Description	Use this command to change the maximum number of BGP4 shared paths, either by setting a value or using the value configured by the ip load-sharing command.	
Usage Guidelines	Use the no form of this command to restore the default.	
Examples	The following example sets the maximum number of BGP4 shared paths to 8. <pre>switch(config)# rbridge-id 10 switch(config-rbridge-id-10)# router bgp switch(config-bgp-router)# address-family ipv4 unicast switch(config-bgp-ipv4u)# maximum-paths 8</pre>	
See Also	ip load-sharing , maximum-paths ebgp ibgp (BGP)	

maximum-paths ebgp ibgp (BGP)

Specifies the number of equal-cost multipath EBGp or IBGP routes or paths that are selected.

Synopsis **maximum-paths** {**ebgp** *num* | **ibgp** *num*}

no maximum-paths

Operands **ebgp** Specifies EBGp routes or paths.

ibgp Specifies IBGP routes or paths.

num The number of equal-cost multipath routes or paths that are selected. Range is from 1 through 8. 1 disables equal-cost multipath.

Defaults This option is disabled.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Enhancements to BGP4 load sharing support the load sharing of BGP4 routes in IP Equal-Cost Multipath (ECMP, even if the BGP4 multipath load-sharing feature is not enabled by means of the **use-load-sharing** option to the **maximum-paths** command. You can set separate values for IGMP and ECMP load sharing. Use this command to specify the number of equal-cost multipath EBGp or IBGP routes or paths that are selected.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples `switch(config)# rbridge-id 10`
 `switch(config-rbridge-id-10)# router bgp`
 `switch(config-bgp-router)# address-family ipv4 unicast`
 `switch(config-bgp-ipv4u)# maximum-paths ebgp 6 ibgp 6`

See Also None

med-missing-as-worst (BGP)

Configures the device to favor a route that has a Multi-Exit Discriminator (MED) over a route that does not have one.

Synopsis **med-missing-as-worst**
 no med-missing-as-worst

Operands None

Defaults This option is disabled.

Command Modes BGP address-family IPv4 unicast configuration mode

Description When MEDs are compared, by default the device favors a low MED over a higher one. Because the device assigns a value of 0 to a route path MED if the MED value is missing, the default MED comparison results in the device favoring the route paths that do not have MEDs. Use this command to configure the device to favor a route that has a Multi-Exit Discriminator (MED) over a route that does not have one.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples Typical example of this command:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-ipv4u)# med-missing-as-worst
```

See Also None

message-interval

Configures the Protocol Independent Multicast (PIM) Join/Prune message interval.

Synopsis **message-interval** *num*
 no message-interval

Operands *num* The interval value in seconds. Valid values range from 10 through 65535 seconds.

Defaults 60 seconds

Command Modes PIM router configuration mode

Description Use this command to specify the interval at which the periodic PIM Join/Prune messages must be sent out.

Usage Guidelines Enter **no message-interval** to disable this feature.

Examples Setting the interval to one hour.

 switch(conf-pim-router)# **message-interval 3600**

See Also **router pim**

metric-type (OSPF)

Configures the default metric type for external routes.

Synopsis **metric-type {type1 | type2}**
no 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.

Defaults **type1**

Command Modes OSPF VRF router configuration mode

Description Use this command to configure the default metric type for external routes.

Usage Guidelines Enter **no metric-type {type1 | type2}** to return to the default setting.

Examples To set the default metric type for external routes to type2:

```
switch# conf t
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# router ospf
switch(config-router-ospf-vrf-default-vrf)# metric-type type2
```

See Also **default-information-originate (OSPF)**

minimum-links

Sets the minimum bandwidth.

Synopsis **minimum-links** *num-of-links*
no minimum-links

Operands *num-of-links* Number of links. Valid values range from 1 through 32.

Defaults 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 Enter **no minimum-links** to restore the default value.

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-lddp)# mode tx
```

To enable only the receive mode:

```
switch(conf-lddp)# mode rx
```

See Also **show lldp interface**

mode (27x40 GbE line card)

Sets Performance or Density operating modes on the 27x40 GbE line card installed in the 8770 Switch.

Synopsis **mode performance**
 no mode performance

Operands None

Defaults Density mode (**no mode performance**) is enabled.

Command Modes port-group

Description Use this command to set Performance or Density (default) operating modes for port groups 1-9 on the 27x40 GbE line card. When a port group is configured in Performance mode, the third port in the port group is persistently disabled, but the remaining two ports operate at up to 40 Gbps in Performance mode to achieve the 80 Gbps maximum rate for the port group. QSFP breakout mode is only supported on ports configured in Performance mode.

If Density mode (default) is configured for a port group, all three ports in the group are enabled in Density mode, so cannot support the 40 Gbps maximum rate. If this mode is configured on all port groups, 27 total ports are available for use.

For more information on port groups and the Performance and Density operating modes on the line card, refer to the “Overview” chapter in the Brocade 8770-4 and 8770-8 Hardware Reference Manuals.

Usage Guidelines Enter **no performance mode** to restore the default value. Power off the line card before configuring operating modes.

Examples To enable Performance mode on port group 9 of the line card in slot 3 of switch with RBridge ID 1.

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# hardware
switch(config-hardware)# port-group 1/3/9
switch(config-port-group-1/3/9)# mode performance
%Warning: port-group mode performance is a disruptive command.
Please save the running-config to startup-config and a power-cycle for the
changes to take place.
```

See Also **port-group, hardware**

modes

Enables and disables operating modes for port groups for Access Gateway mode.

Synopsis **modes** *mode_name*
 no mode *mode_name*

Operands *mode_name* **lb** (Automatic Login Balancing)

Defaults **lb**

Command Modes Port Grouping configuration

Description Enables or disables operating modes for a specific port group. Login Balancing (LB) is the only mode that you can enable. Automatic Login Balancing is enabled by default for a port group when the port group is created. If LB mode is enabled for a port group and a VF_Port goes offline, logins in the port group are redistributed among the remaining VF_Ports. Similarly, if an N_Port comes online, port logins in the port group are redistributed to maintain a balanced N_Port-to-VF_Port ratio.

Usage Guidelines You must be in Port Grouping configuration mode for a specific port group to use this command. Entering **no modes** *mode name* disables the mode.

Consider the following when using LB mode with **show running-config ag** and **show ag** commands:

- The only Port Grouping mode that you can enable or disable is LB mode.
- When LB mode is disabled in a port group, the **show running-config ag**, **show ag map**, and **show ag** commands display the *configured* VF_Port to N_Port mapping. This is because configured and active mapping are the same.
- When LB mode is enabled in a port group, **show ag** and **show ag map** displays the active mapping only because VF_Port to N_Port mapping is based on the current distributed load across all N_Ports. The **show running-config ag** command displays the configured mapping only.

Examples Enable Automatic Login Balancing mode on port group 8.

```
sw0(config-rbridge-id-3-ag-pg-8)# modes lb
```

Disable Automatic Login Balancing mode on port group 8.

```
sw0(config-rbridge-id-3-ag-pg-8)# no modes lb
```

See Also None

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. Valid values range from 0 through 511 in logical chassis mode, 0 through 23 for standalone mode.

Defaults None

Command Modes Global configuration mode

Description Use this command to enable a session for monitoring traffic.

Usage Guidelines The source and destination ports must be in the same port-group on a Brocade VDX 6720-60.
Enter **no monitor session** to delete the port mirroring session.

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**

monitor-session (VXLAN gateway)

Enables switched port analyzer (SPAN) on one or all tunnels of this gateway.

Synopsis **monitor session** *session_number* **direction** { **tx** | **rx** | **both** } [**remote-endpoint** { *ip_address* | **any** }]
vlan [**add** | **remove**] *VLAN_ID_range*
no monitor session *session_number*

Operands	<i>session_number</i>	Specifies the SPAN session ID that was configured with the global monitor session command.
	tx	Enables SPAN for the transmitting tunnels.
	rx	Enables SPAN for the receiving tunnels.
	both	Enables SPAN for both the transmitting and receiving tunnels.
	<i>ip_address</i>	Enables SPAN for the specified the IPv4 address of the remote hypervisor NSX VXLAN termination endpoint (VTEP).
	any	Enables SPAN for all tunnels on the gateway.
	add	Enables SPAN on specified VLAN IDs. You can use this option if you have disabled SPAN on specific VLAN IDs and now want to re-enable SPAN on these IDs.
	remove	Disables SPAN on specified VLAN IDs.
	<i>VLAN_ID_range</i>	Specifies the VLAN IDs for enabling SPAN.

Defaults None

Command Modes VXLAN Gateway Configuration mode

Description Use this command to enable SPAN on one or all tunnels of this gateway for specified VLANs. You can use the *remote-endpoint* option to choose all tunnels or specific tunnels of this gateway. You choose a specific tunnel by specifying the remote hypervisor VTEP IP address. This address is matched with the destination IP address of the tunnels.

The *remove* option can be used to exclude VLANs from a previously configured list. If all the VLANs are removed, the entire SPAN configuration is deleted (this is the same behavior as running the **no monitor session session_number** command).

The only way to change the direction once you have run this command is to remove the SPAN configuration, then rerun the **monitor session** command.

Usage Guidelines Specified VLANs must already be configured as exported through this gateway.

The SPAN session number must already be configured, and the SPAN destination must already be specified and cannot be a tunnel.

The SPAN session must not include source port configuration for this gateway.

The deletion of an attached VLAN (by using the **no attach vlan** command) is blocked if SPAN has been enabled for the VLAN you are trying to delete.

The **no** form of this command removes SPAN configuration for the gateway.

Examples To enable SPAN for all tunnels in both directions for VLAN IDs 1 through 10 and SPAN session ID 3:

```
switch# configure  
switch(config)# overlay-gateway gateway1  
switch(config-overlay-gw-gateway1)# monitor session 3 direction both  
remote-endpoint any vlan add 1-10
```

See Also

mtu

Specifies the size of the maximum transmission unit (MTU) on an interface.

Synopsis `mtu size`

Operands `size` Size, in bytes, of the MTU. Range is from 1522 through 9216.

Defaults 10-Gbps Ethernet interfaces have a default MTU of 2500 bytes.

Command Modes Interface configuration mode

Description Use this command to specify the MTU on an interface.

Usage Guidelines Configuring an MTU on a VLAN interface is not valid.

Examples None

See Also None

multipath (BGP)

Changes load sharing to apply to only IBGP or EBGp paths, or to support load sharing among paths from different neighboring autonomous systems (ASs).

Synopsis **multipath** [**ebgp** | **ibgp** | **multi-as**]
no multipath

Operands **ebgp** Enables load sharing of EBGp paths only.
ibgp Enables load sharing of IBGP paths only.
multi-as Enables load sharing of paths from different neighboring autonomous systems.

Defaults This option is disabled.

Command Modes BGP address-family IPv4 unicast configuration mode

Description By default, when BGP4 load sharing is enabled, both IBGP and EBGp paths are eligible for load sharing, while paths from different neighboring autonomous systems are not. Use this command to change load sharing to apply to only IBGP or EBGp paths, or to support load sharing among paths from different neighboring autonomous systems.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To change load sharing to apply to both EBGp and IBGP paths:

```

switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# multipath ebgp ibgp

```

See Also None

multiplier (LLDP)

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. Valid values range from 2 through 10.

Defaults Multiplier default 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.

Usage Guidelines Enter **no multiplier** to return to the default setting.

Examples To set the number of consecutive misses:

 `switch(conf-lddp) # multiplier 2`

See Also **hello (LLDP)**

multiplier (UDLD)

Sets timeout multiplier for missed UDLD PDUs.

Synopsis **multiplier** *value*
 no multiplier

Operands *value* Specifies a multiplier value to use. Valid values range from 3 through 10.

Defaults Multiplier default value is 5.

Command Modes Protocol UDLD configuration mode

Description Use this command to set the timeout multiplier for missed UDLD PDUs. The timeout interval is the product of the "hello" time interval at the other end of the link and the "multiplier" value. When the UDLD protocol times out waiting for UDLD PDUs, it will block the port.

When the device at one end is a Brocade IP product, the timeout interval is the product of the "hello" time interval at the other end and the "multiplier" value.

When the UDLD protocol times out waiting for UDLD PDUs, it will block the port.

Usage Guidelines Enter **no multiplier** to return to the default setting.

Examples To set the multiplier to 8:

```
switch(config)# protocol udld  
switch(config-udld)# multiplier 8
```

See Also **hello (UDLD)**

nas auto-qos

Enables the Quality of Service (QoS) functionality for the Auto-NAS (automatic network attached storage) feature.

Synopsis **nas auto-qos**
 no nas auto-qos

Operands None

Defaults None

Command Modes Global configuration mode

Description Use this command to enable or disable the QoS functionality for Auto-NAS.

Usage Guidelines This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Use the **no** form of this command to disable the Auto-NAS feature.

Examples None

See Also **backup-advertisement-interval, clear nas statistics, nas server-ip, show nas statistics, show running-config nas server-ip, show system internal nas, show cee maps**

nas server-ip

Identifies the port that is to receive Auto NAS (automatic network attached storage) traffic.

Synopsis **nas server-ip** *address/prefix* [**vlan** *vlan_ID* | **vrf** *vrf_name*]
no nas server-ip *address*

Operands *address/prefix* IP address/prefix to receive NAS traffic.
 vlan *vlan_ID* VLAN ID.
 vrf *vrf_name* VRF name.

Defaults None

Command Modes Global configuration mode

Description Use this command to specify or disable the Auto NAS server-ip prefix.

Usage Guidelines This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.
 Use the **no** form of this command to remove a nas server-ip prefix..

Examples To identify an IP address/prefix of 2.2.2.2/32 to receive NAS traffic over VLAN 10:

```
switch# configure  
switch(config)# nas server-ip 2.2.2.2/32 vlan 10
```

See Also **clear nas statistics, nas auto-qos, show nas statistics, show running-config nas server-ip, show system internal nas, show cee maps**

nbr-timeout

Configures the neighbor timeout interval.

Synopsis **nbr-timeout** *num*
 no nbr-timeout

Operands *num* Interval value in seconds. Valid values range from 35 through 12600 seconds.

Defaults The default is 105.

Command Modes PIM router configuration mode

Description Use this command to specify the interval after which a neighbor is considered to be absent.

Usage Guidelines Enter **no nbr-timeout** to disable this feature.

Examples Setting the timeout to 600 seconds.

 `switch(conf-pim-router)# nbr-timeout 600`

See Also **router pim**

neighbor (BGP)

Assigns a neighbor to a specified IPv4 address or peer group to provide a variety of configuration options.

Synopsis **neighbor** {*ip-address* | *peer-group-name*}
 {advertisement-interval | as-override | capability | description | ebgp-multihop |
 enforce-first-as | local-as | maxas-limit | next-hop-self | password | peer-group | remote-as |
 remove-private-as | shutdown | soft-reconfiguration | timers | update-source}

 no neighbor {*ip-address* | *peer-group-name*}
 {advertisement-interval | as-override | capability | description | ebgp-multihop |
 enforce-first-as | local-as | maxas-limit | next-hop-self | password | peer-group | remote-as |
 remove-private-as | shutdown | soft-reconfiguration | timers | update-source}

Operands	<i>ip-address</i>	IPv4 address of the neighbor
	<i>peer-group-name</i>	Alphanumeric characters. Range is from 1 through 63.
	advertisement-interval	See neighbor advertisement-interval (BGP) .
	as-override	See neighbor as-override (BGP) .
	capability	See neighbor capability as4 (BGP) .
	description	See neighbor description (BGP) .
	ebgp-multihop	See neighbor ebgp-multihop (BGP) .
	enforce-first-as	See neighbor enforce-first-as (BGP) .
	local-as	See neighbor local-as (BGP) .
	maxas-limit	See neighbor maxas-limit in (BGP) .
	next-hop-self	See neighbor next-hop-self (BGP) .
	password	See neighbor password (BGP) .
	peer-group	See neighbor peer-group (BGP) .
	remote-as	See neighbor remote-as (BGP) .
	remote-private-as	See neighbor remove-private-as (BGP) .
	shutdown	See neighbor shutdown (BGP) .
	soft-reconfiguration	See neighbor soft-reconfiguration inbound (BGP) .
	timers	See neighbor timers (BGP) .
	update-source	See neighbor update-source (BGP) .

Defaults None

Command Modes BGP configuration mode
 BGP address-family IPv4 unicast configuration mode

2 neighbor (BGP)

Description Use this command to assign a neighbor to a specified peer group to provide a variety of configuration options. Neighbor configuration appears in both BGP global and BGP Address-Family command modes. The neighbor parameters/attributes that are common to all of the address families appear in the global mode, making support available for IPv6 address families in the future. The neighbor parameters/attributes that are specific to the address-family appear within the address-family submode.

Usage Guidelines Use the **no** form of this command to remove the neighbor from the specified peer group or remove an option.

Examples To assign a neighbor to a specified peer group and view available options:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# neighbor 10.11.12.13 ?
Possible completions:
  advertisement-interval  Minimum interval between sending BGP routing updates
  as-override             Override matching AS-number while sending update
  capability              Advertise capability to the peer
  description             Neighbor by description
  ebgp-multihop           Allow EBGp neighbors not on directly connected
                          networks
  enforce-first-as        Enforce the first AS for EBGp routes
  local-as               Assign local-as number to neighbor
  maxas-limit             Impose limit on number of ASes in AS-PATH attribute
  next-hop-self           Disable the next hop calculation for this neighbor
  password               Enable TCP-MD5 password protection
  peer-group              Create Peer Group
  remote-as               Specify a BGP neighbor
  remove-private-as       Remove private AS number from outbound updates
  shutdown                Administratively shut down this neighbor
  soft-reconfiguration    Per neighbor soft reconfiguration
  timers                  BGP per neighbor timers
  update-source           Source of routing updates
```

See Also All BGP neighbor commands listed under Operands.

neighbor (OSPF)

Manually configures a neighbor.

Synopsis **neighbor** *A.B.C.D*
 no neighbor

Operands *A.B.C.D* IPv4 address of the neighbor.

Defaults Neighbors are not configured.

Command Modes OSPF VRF router configuration mode

Description Use this command to manually configure a neighbor. It is typically used in point-to-point networks.

Usage Guidelines OSPF Hellos must use a unicast address, not broadcast or multicast packets.
Enter **no neighbor** *A.B.C.D* to remove the specified neighbor.

Examples To configure a neighbor whose IPv4 address is 1.1.1.1:

```
switch(config)# rbridge-id 5  
switch(config-rbridge-id-5)# router ospf  
switch(config-router-ospf-vrf-default-vrf)# neighbor 1.1.1.1
```

See Also None

neighbor advertisement-interval (BGP)

Enables changes to interval over which a specified neighbor or peer-group holds route updates before forwarding them.

Synopsis **neighbor** *{ip-address | peer-group-name}* **advertisement-interval** *seconds*
no neighbor

Operands *ip-address* IPv4 address of the neighbor
peer-group-name Peer group name configured by the **neighbor peer-group-name** command.
seconds Range is from 0 through 3600.

Defaults The default is 0.

Command Modes BGP configuration mode

Description Use this command to configure the interval, in seconds, over which a specified neighbor or peer group holds all route updates before forwarding them. When the timer expires, the routes are sent as a batch.

Usage Guidelines None
 Use the **no** form of this command to reset the interval to the default.

Examples `switch(config)# rbridge-id 10`
 `switch(config-rbridge-id-10)# router bgp`
 `switch(config-bgp-router)# neighbor 10.11.12.13 advertisement-interval 60`

See Also None

neighbor as-override (BGP)

Replaces the autonomous system number (ASN) of the originating router with the ASN of the sending BGP router.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **as-override**
no neighbor as-override

Operands *ip-address* IPv4 address of the neighbor
 peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.

Defaults None

Command Modes BGP configuration mode

Description BGP loop prevention verifies the ASN in the AS path. If the receiving router sees its own ASN in the AS path of the received BGP packet, the packet is dropped. The receiving router assumes that the packet originated from its own AS and has reached the place of origination. This can be a significant problem if the same ASN is used among various sites, preventing sites with identical ASNs from being linked by another ASN. In this case, routing updates are dropped when another site receives them.

Use this command to replace the ASN of the originating router with the ASN of the sending BGP router.

Usage Guidelines Use the **no** form of this command to disable this feature.

Examples To change an advertisement interval:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# neighbor 10.11.12.13 as-override
```

See Also None

neighbor capability as4 (BGP)

Enables or disables support for 4-byte autonomous system numbers (ASNs) at the neighbor or peer-group level.

Synopsis **neighbor** *{ip-address | peer-group-name}* **capability as4** [**enable** | **disable**]
no neighbor capability as4

Operands

<i>ip-address</i>	IPv4 address of the neighbor
<i>peer-group-name</i>	Peer group name configured by the neighbor peer-group-name command.
enable	Enables 4-byte numbering.
disable	Disables 4-byte numbering.

Defaults Four-byte ASNs are disabled by default.

Command Modes BGP configuration mode

Description Use this command to enable 4-byte ASNs at the neighbor or peer-group level.

Usage Guidelines 4-byte ASNs are first considered at the neighbor, then at the peer group, and finally at the global level.

Use the **disable** keyword or the **no** form of this command to remove all neighbor capability for AS4.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# neighbor 10.11.12.13 capability as4 enable
```

See Also None

neighbor default-originate (BGP)

Configures the device to send the default route 0.0.0.0 to a neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **default-originate** {**route-map** *map-name*}
no neighbor

Operands

<i>ip-address</i>	IPv4 address of the neighbor
<i>peer-group-name</i>	Peer group name configured by the neighbor <i>peer-group-name</i> command.
route-map	Optionally injects the default route conditionally, depending on the match conditions in the route map.
<i>map-name</i>	Name of the route map.

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to configure the device to send the default route 0.0.0.0 to a neighbor.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# neighbor 10.11.12.13 default-originate route-map
myroutemap
```

See Also **route-map**

neighbor description (BGP)

Specifies a name for a neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **description** *string*
no neighbor {*ip-address* | *peer-group-name*} **description** *string*

Operands *ip-address* IPv4 address of the neighbor
peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.
description *string* Specifies the name of the neighbor, an alphanumeric string up to 220 characters long.

Defaults None

Command Modes BGP configuration mode

Description Use this command to describe a neighbor.

Usage Guidelines Use the **no** form of this command to remove the name.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **neighbor 10.11.12.13 description mygoodneighbor**

See Also None

neighbor ebgp-multihop (BGP)

Allows EBGp neighbors that are not on directly connected networks and sets an optional maximum hop count.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **ebgp-multihop** [*max-hop-count*]
no neighbor {*ip-address* | *peer-group-name*} **ebgp-multihop**

Operands *ip-address* IPv4 address of the neighbor
 peer-group-name Peer group name configured by the **neighbor peer-group-name** command.
 max-hop-count Maximum hop count (optional). Range is from 1 through 255.

Defaults None

Command Modes BGP configuration mode

Description Use this command to allow EBGp neighbors that are not on directly connected networks and set an optional maximum hop count

Usage Guidelines Use the **no** form of this command to disable this feature.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **neighbor 10.11.12.13 ebgp-multihop 20**

See Also None

neighbor enforce-first-as (BGP)

Ensures that a device requires the first ASN listed in the AS_SEQUENCE field of an AS path-update message from EBGp neighbors to be the ASN of the neighbor that sent the update.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **enforce-first-as** [**enable** | **disable**]
no neighbor {*ip-address* | *peer-group-name*} **enforce-first-as** [**enable** | **disable**]

Operands

<i>ip-address</i>	IPv4 address of the neighbor
<i>peer-group-name</i>	Peer group name configured by the neighbor <i>peer-group-name</i> command.
enable	Enables this feature.
disable	Disables this feature.

Defaults This feature is disabled: A device does not require the first ASN listed in the AS_SEQUENCE field of an AS path-update message from EBGp neighbors to be the ASN of the neighbor that sent the update.

Command Modes BGP configuration mode

Description Use this command to ensure that a device requires the first ASN listed in the AS_SEQUENCE field of an AS path-update message from EBGp neighbors to be the ASN of the neighbor that sent the update.

Usage Guidelines Use the **no** form of this command to disable this requirement globally for the device.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# neighbor 10.11.12.13 enforce-first-as enable
```

See Also None

neighbor filter-list (BGP)

Specifies a filter list to be applied to updates from or to the specified neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **filter-list** *ip-prefix-list-name* [**in** | **out**]
no neighbor {*ip-address* | *peer-group-name*} **filter-list** *ip-prefix-list-name* [**in** | **out**]

Operands

<i>ip-address</i>	IPv4 address of the neighbor
<i>peer-group-name</i>	Peer group name configured by the neighbor <i>peer-group-name</i> command.
<i>ip-prefix-list-name</i>	Name of the filter list.
in	Specifies that the list is applied on updates received from the neighbor.
out	Specifies that the list is applied on updates sent to the neighbor.

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to specify a filter list to be applied to updates from or to the specified neighbor.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# neighbor 10.11.12.13 filter-list myfilterlist out
```

See Also None

neighbor local-as (BGP)

Causes the device to prepend the local autonomous system number (ASN) automatically to routes received from an EBGp peer.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **local-as** *num* {**no-prepend**}
no neighbor {*ip-address* | *peer-group-name*} **local-as** *num* {**no-prepend**}

Operands *ip-address* IPv4 address of the neighbor
 peer-group-name Peer group name configured by the **neighbor peer-group-name** command.
 num Local ASN. Range is from 1 through 4294967295.
 no-prepend Causes the device to stop pre-pending the selected ASN.

Defaults None

Command Modes BGP configuration mode

Description Use this command to causes the device to prepend the local autonomous system number (ASN) automatically to routes received from an EBGp peer.

Usage Guidelines Use the **no** form of this command to remove the local ASN.

Examples To ensure that a device prepends the local ASN:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# neighbor 10.11.12.13 local-as 100
```

To stop the device from pre-pending the selected ASN:

```
switch(config-bgp-router)# neighbor 10.11.12.13 local-as 100 no-prepend
```

See Also None

neighbor maxas-limit in (BGP)

Causes the device to discard routes received in UPDATE messages if those routes exceed a maximum AS path length.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **maxas-limit in** {*num* | **disable**}
no neighbor {*ip-address* | *peer-group-name*} **maxas-limit in** {*num* | **disable**}

Operands

<i>ip-address</i>	IPv4 address of the neighbor
<i>peer-group-name</i>	Peer group name configured by the neighbor peer-group-name command.
<i>num</i>	Maximum length of the AS path. Range is from 0 through 300.
disable	Prevents a neighbor from inheriting the configuration from the peer group or global configuration and instead uses the default system value.

Defaults The default for *num* is 300.

Command Modes BGP configuration mode

Description Use this command to cause the device to discard routes received in UPDATE messages if those routes exceed a maximum AS path length.

Usage Guidelines Use the **no** form of this command to remove this configuration at the global level.

Examples To change the length of the maximum allowed AS path length from the default:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# neighbor 10.11.12.13 maxas-limit in 200
```

To prevent a neighbor from inheriting the configuration from the peer group or global configuration and instead use the default system value:

```
switch(config-bgp-router)# neighbor 10.11.12.13 maxas-limit in disable
```

See Also None

neighbor maximum-prefix (BGP)

Specifies the maximum number of IP network prefixes (routes) that can be learned from a specified neighbor or peer group.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **maximum-prefix** *num* [*threshold*] [**teardown**]
no neighbor {*ip-address* | *peer-group-name*} **maximum-prefix** *num* [*threshold*] [**teardown**]

Operands

<i>ip-address</i>	IPv4 address of the neighbor
<i>peer-group-name</i>	Peer group name configured by the neighbor <i>peer-group-name</i> command.
<i>num</i>	Maximum number of IP prefixes that can be learned. Range is from 0 through 4294967295. Default is 0 (unlimited).
<i>threshold</i>	Specifies the percentage of the value specified by <i>num</i> that causes a syslog message to be generated. Range is from 1 through 100. Default is 100.
teardown	Tears down the neighbor session if the maximum number of IP prefixes is exceeded.

Defaults See Operands.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to specify the maximum number of IP network prefixes (routes) that can be learned from a specified neighbor or peer group.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# neighbor 10.11.12.13 prefix-list 100000 threshold 80
```

See Also None

neighbor next-hop-self (BGP)

Causes the device to list itself as the next hop in updates that are sent to the specified neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **next-hop-self** [**always**]
no neighbor {*ip-address* | *peer-group-name*} **next-hop-self** [**always**]

Operands *ip-address* IPv4 address of the neighbor
 peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.
 always Enables this feature for route reflector (RR) routes.

Defaults None

Command Modes BGP configuration mode

Description Use this command to cause the device to list itself as the next hop in updates that are sent to the specified neighbor.

Usage Guidelines Use the **no** form of this command to remove this configuration at the global level.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **neighbor 10.11.12.13 next-hop-self**

See Also None

neighbor password (BGP)

Specifies an MD5 password for securing sessions between the device and a neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **password** *string*
no neighbor {*ip-address* | *peer-group-name*} **password** *string*

Operands *ip-address* IPv4 address of the neighbor
 peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.
 string Alphanumeric characters. Range is from 1 through 63.

Defaults None

Command Modes BGP configuration mode

Description Use this command to specify an MD5 password between the device and a neighbor.

Usage Guidelines Use the **no** form of this command to remove this configuration at the global level.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **neighbor 10.11.12.13 password s0M3P@55W0Rd**

See Also None

neighbor peer-group (BGP)

Enables the creation of a BGP peer group.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **peer-group** *string*
no neighbor {*ip-address* | *peer-group-name*} **peer-group** *string*

Operands *ip-address* IPv4 address of the neighbor
 peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.
 string Alphanumeric characters. Range is from 1 through 63.

Defaults None

Command Modes BGP configuration mode

Description Use this command to create a BGP peer group.

Usage Guidelines Use the **no** form of this command to remove the peer group.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **neighbor 10.11.12.13 peer-group mypeergroup1**

See Also None

neighbor prefix-list (BGP)

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to IP address and mask length.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **prefix-list** *string* {**in** | **out**}
no neighbor {*ip-address* | *peer-group-name*} **prefix-list** *string* {**in** | **out**}

Operands

<i>ip-address</i>	IPv4 address of the neighbor
<i>peer-group-name</i>	Peer group name configured by the neighbor <i>peer-group-name</i> command.
<i>string</i>	Name of the prefix list.
in	Applies the filter in oncoming routes.
out	Applies the filter in outgoing routes.

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to filter the outgoing and incoming route updates to or from a particular BGP neighbor according to IP address and mask length.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# neighbor 10.11.12.13 prefix-list myprefixlist in
```

See Also None

neighbor remote-as (BGP)

Specifies the autonomous system (AS) in which a remote neighbor resides.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **remote-as** *num*
no neighbor {*ip-address* | *peer-group-name*} **remote-as** *num*

Operands *ip-address* IPv4 address of the neighbor
 peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.
 num Remote AS number (ASN). Range is from 1 through 4294967295.

Defaults None

Command Modes BGP configuration mode

Description Use this command to specify the AS in which a remote neighbor resides.

Usage Guidelines Use the **no** form of this command to remove the neighbor from the AS.

Examples switch(config)# **rbridge-id** 10
 switch(config-rbridge-id-10)# **router** **bgp**
 switch(config-bgp-router)# **neighbor** 10.11.12.13 **remote-as** 100

See Also None

neighbor remove-private-as (BGP)

Configures a device to remove private autonomous system numbers (ASNs) from UPDATE messages that the device sends to a neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **remove-private-as**
no neighbor {*ip-address* | *peer-group-name*} **remove-private-as**

Operands *ip-address* IPv4 address of the neighbor
peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.

Defaults None

Command Modes BGP configuration mode

Description Use this command to configure a device to remove private autonomous system numbers (ASNs) from UPDATE messages that the device sends to a neighbor. The device will remove ASNs 64512 through 65535 (the well-known BGP4 private ASNs) from the AS-path attribute in UPDATE messages that the device sends to a neighbor.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples `switch(config)# rbridge-id 10`
`switch(config-rbridge-id-10)# router bgp`
`switch(config-bgp-router)# neighbor 10.11.12.13 remove-private-as`

See Also None

neighbor route-map (BGP)

Filters the outgoing and incoming route updates to or from a particular BGP neighbor according to a set of attributes.

Synopsis **neighbor** *{ip-address | peer-group-name}* **route-map** *string* **{in | out}**
no neighbor *{ip-address | peer-group-name}* **route-map** *string* **{in | out}**

Operands

<i>ip-address</i>	IPv4 address of the neighbor
<i>peer-group-name</i>	Peer group name configured by the neighbor <i>peer-group-name</i> command.
<i>string</i>	Name of the route map.
in	Applies the filter on incoming routes.
out	Applies the filter on outgoing routes.

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to filter the outgoing and incoming routes to or from a particular BGP neighbor according to a set of attributes defined in a route map.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# neighbor 10.11.12.13 route-map myroutemap out
```

See Also **route-map**

neighbor route-reflector-client (BGP)

Configures a neighbor to be a route-reflector client.

Synopsis **neighbor** {*ip* | *peer-group*} **route-reflector-client**
no neighbor {*ip* | *peer-group*} **route-reflector-client**

Operands *ip* IPv4 address in dotted-decimal notation.
 peer-group Peer group name configured by the **neighbor** *peer-group-name* command.

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command on a host device to configure a neighbor to be a route-reflector client. Once configured, the host device from which the configuration is made acts as a route-reflector server.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **address-family ipv4 unicast**
 switch(config-bgp-ipv4u)# **neighbor 10.11.12.13 route-reflector-client**

See Also None

neighbor send-community (BGP)

Enables sending the community attribute in updates to the specified BGP neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **send-community** {**both** | **extended** | **standard**}
no neighbor {*ip-address* | *peer-group-name*} **send-community** {**both** | **extended** | **standard**}

Operands

<i>ip-address</i>	IPv4 address of the neighbor
<i>peer-group-name</i>	Peer group name configured by the neighbor <i>peer-group-name</i> command.
both	Sends both standard and extended attributes.
extended	Sends extended attributes.
standard	Sends standard attributes.

Defaults The device does not send community attributes.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to send the community attribute in updates to the specified BGP neighbor.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# neighbor 10.11.12.13 send-community standard
```

See Also **route-map**

neighbor shutdown (BGP)

Causes a device to shut down the session administratively with its neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **shutdown** {**generate-rib-out**}
no neighbor {*ip-address* | *peer-group-name*} **shutdown** {**generate-rib-out**}

Operands *ip-address* IPv4 address of the neighbor
peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.
generate-rib-out When a peer is put into shutdown state, Routing Information Base (RIB) outbound routes are not produced for that peer. Use this option to produce those routes.

Defaults None

Command Modes BGP configuration mode

Description Shutting down a session lets you configure the neighbor and save the configuration without the need to establish a session with that neighbor.

Usage Guidelines Use the **no** form of this command to restore the defaults.

Examples To cause a device to shut down the session administratively with its neighbor:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# neighbor 10.11.12.13 shutdown
```

To do the above and generate RIB outbound routes:

```
switch(config-bgp-router)# neighbor 10.11.12.13 shutdown generate-rib-out
```

See Also None

neighbor soft-reconfiguration inbound (BGP)

Stores all the route updates received from a neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**
no neighbor {*ip-address* | *peer-group-name*} **soft-reconfiguration inbound**

Operands *ip-address* IPv4 address of the neighbor
 peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.

Defaults None

Command Modes BGP configuration mode

Description Soft reconfiguration stores all the route updates received from a neighbor. If you request a soft reset of inbound routes, the software compares the policies against the stored route updates, instead of requesting the neighbor's BGP4 route table or resetting the session with the neighbor.

Usage Guidelines Use the **no** form of the command to disable this feature.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **neighbor 10.11.12.13 soft-reconfiguration inbound**

See Also None

neighbor timers (BGP)

Specifies how frequently a device sends KEEPALIVE messages to its BGP4 neighbors, as well as how long the device waits for KEEPALIVE or UPDATE messages before concluding that a neighbor is dead.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **timers** {**keep-alive** *time1*} {**hold-time** *time2*}
no neighbor {*ip-address* | *peer-group-name*} **timers** {**keep-alive** *time1*} {**hold-time** *time2*}

Operands *ip-address* IPv4 address of the neighbor
peer-group-name Peer group name configured by the **neighbor peer-group-name** command.
time1 Keep-alive timer. Range is from 0 through 65535 seconds.
time2 Hold timer. Range is from 0 through 65535 seconds.

Defaults The default for *time1* is 60. The default for *time2* is 180.

Command Modes BGP configuration mode

Description Use this command to specify how frequently a device sends KEEPALIVE messages to its BGP4 neighbors, as well as how long the device waits for KEEPALIVE or UPDATE messages before concluding that a neighbor is dead.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# neighbor 10.11.12.13 timers keep-alive 120
hold-time 360
```

See Also None

neighbor unsuppress-map (BGP)

Removes route suppression from neighbor routes when those routes have been suppressed as a result of aggregation.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **unsuppress-map** *string*
no neighbor {*ip-address* | *peer-group-name*} **unsuppress-map** *string*

Operands *ip-address* IPv4 address of the neighbor.
 peer-group-name Peer group name configured by the **neighbor** *peer-group-name* command.
 string Name of the route map.

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to remove route suppression from neighbor routes when those routes have been suppressed as a result of aggregation. All routes matching route-map rules are unsuppressed.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples switch(config)# **rbridge-id** 10
 switch(config-rbridge-id-10)# **router** **bgp**
 switch(config-bgp-router)# **address-family** **ipv4** **unicast**
 switch(config-bgp-ipv4u)# **neighbor** 10.11.12.13 **unsuppress-map** myroutemap

See Also route-map

neighbor update-source (BGP)

Configures the device to communicate with a neighbor through a specified interface.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **update-source** *ip-addr* | {**tengigabitethernet** | **gigabitethernet** | **fortygigabitethernet**} *rbridge-id/slot/portnum* | **loopback** *num* | **ve-interface** *vlan_id*]

no neighbor {*ip-address* | *peer-group-name*} **update-source** *ip-addr* | {**tengigabitethernet** | **gigabitethernet** | **fortygigabitethernet**} *rbridge-id/slot/portnum* | **loopback** *num* | **ve-interface** *vlan_id*]

Operands	<i>ip-address</i>	IPv4 address of the neighbor
	<i>peer-group-name</i>	Peer group name configured by the neighbor <i>peer-group-name</i> command.
	<i>ip-addr</i>	IP address of the update source.
	tengigabitethernet	10-gigabit Ethernet interface
	gigabitethernet	1-gigabit Ethernet interface
	fortygigabitethernet	40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Routing bridge ID
	<i>slot</i>	Slot number
	<i>portnum</i>	Port number
	loopback <i>num</i>	Specifies a loopback interface.
	ve-interface <i>vlan_id</i>	Specifies a virtual Ethernet VLAN interface. Refer to the Usage Guidelines.

Defaults None

Command Modes BGP configuration mode

Description Use this command to configure the device to communicate with a neighbor through a specified interface.

Usage Guidelines Use the **no** form of the command to restore the defaults.

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).

Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples Typical command example.

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# neighbor 10.11.12.13 update-source
10.11.12.14tengigabitethernet 15/1/1
```

See Also None

neighbor weight (BGP)

Specifies a weight that the device will add to routes that are received from the specified BGP neighbor.

Synopsis **neighbor** {*ip-address* | *peer-group-name*} **weight** *num*
no neighbor {*ip-address* | *peer-group-name*} **weight** *num*

Operands *ip-address* IPv4 address of the neighbor.
 peer-group-name Name of the peer group.
 num Value from 1 through 65535.

Defaults The default for *num* is 0.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to specify a weight that the device will add to routes that are received from the specified BGP neighbor. BGP4 prefers larger weights over smaller weights.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples `switch(config)# rbridge-id 10`
 `switch(config-rbridge-id-10)# router bgp`
 `switch(config-bgp-router)# address-family ipv4 unicast`
 `switch(config-bgp-ipv4u)# neighbor 10.11.12.13 weight 100`

See Also None

network (BGP)

Configures the device to advertise a network.

Synopsis **network** *network/mask* [**route-map** *map-name*] | [**weight** *num*] | [**backdoor**]
no network *network/mask* [**route-map** *map-name*] | [**weight** *num*] | [**backdoor**]

Operands

<i>network/mask</i>	Network and mask in CIDR notation.
<i>map-name</i>	Name of the route map with which to set or change BGP4 attributes for the network to be advertised.
<i>num</i>	Weight to be added to routes to this network. Range is 0 through 65535.
backdoor	Changes administrative distance of the route to this network from the EBGp administrative distance (the default is 20) to the local BGP4 weight (the default is 200), tagging the route as a backdoor route.

Defaults The default for *num* is 0.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to configure the device to advertise a network. BGP4 prefers larger weights over smaller weights.

Usage Guidelines Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# network 10.11.12.13/30 route-map myroutemap
```

See Also **route-map**

next-hop-enable-default (BGP)

Configures the device to use the default route as the next hop.

Synopsis **next-hop-enable-default**
 no next-hop-enable-default

Operands None

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to configure the device to use the default route as the next hop.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples `switch(config)# rbridge-id 10`
 `switch(config-rbridge-id-10)# router bgp`
 `switch(config-bgp-router)# address-family ipv4 unicast`
 `switch(config-bgp-ipv4u)# next-hop-enable-default`

See Also None

next-hop-recursion (BGP)

Enables recursive next-hop lookups.

Synopsis **next-hop-recursion**
 no next-hop-recursion

Operands None

Defaults None

Command Modes BGP address-family IPv4 unicast configuration mode

Description If the BGP4 next hop is not the immediate next hop, a recursive route lookup in the IP routing information base (RIB) is needed. With recursion, a second routing lookup is required to resolve the exit path for destination traffic. Use this command to enable recursive next-hop lookups.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **address-family ipv4 unicast**
 switch(config-bgp-ipv4u)# **next-hop-recursion**

See Also None

nport

Enables N_Port configuration mode for a specific N_Port ID for Access Gateway mode.

Synopsis **nport** *port*
 no nport *port*

Operands *port* N_Port number supported by hardware platform.

Defaults None

Command Modes Access Gateway (AG) configuration

Description This command enables N_Port configuration mode for a specific N_Port number so that you can map VF_Ports to the N_Port (Port Mapping).

Usage Guidelines To use this command, you must be in Access Gateway (AG) configuration mode. This command enables N_Port configuration mode for the specific N_Port. While in this mode, you can map VF_Ports to the N_Port. Enter the N_Port in RBridge ID/port group ID/N_Port ID format, such as 3/0/4 for Rbridge 3, port group 0 (default port group), and N_Port 4.

Examples Enabling N_Port configuration mode for N_Port 4 while in AG configuration mode.

```
sw0(config-rbridge-id-2-ag)# nport 2/0/4  
sw0(config-rbridge-id-2-ag-nport-if-fi-2/0/4)#
```

See Also **show ag, map fport interface fcoe**

nport interface Fibrechannel

Adds or deletes N_Ports in a specified port group for Access Gateway mode.

Synopsis **nport interface Fibrechannel** *port*
 no nport interface Fibrechannel *port*

Operands *port* N_Port number supported by switch model.

Defaults None

Command Modes Port Grouping configuration mode

Description Adds or deletes N_Ports in a port group.

Usage Guidelines To use this command, you must be in Port Grouping configuration mode for a specific port group. Before adding an N_Port to a port group, you must remove the N_Port from its current port group unless the port resides in default port group 0 (pg 0). N_Ports are identified by the format *rbridge-id/slot/N_Port*, such as 3/0/4 for RBridge 3, slot 0, and N_Port 4.

Examples Adding N_Port 3/0/3 to port group 2 (pg 2):
 sw0(config-rbridge-id-3-ag-pg-2)# **nport interface Fibrechannel 3/0/3**
 Removing N_Port 3/0/3 from port group 3 (pg 3)
 sw0(config-rbridge-id-3-ag-pg-3)# **nport interface Fibrechannel 3/0/3**

See Also **pg, show ag pg**

nssa-translator (OSPF)

Configures Not So Stubby Area (NSSA) Type 7-to-Type 5 Link State Advertisement (LSA) translation.

Synopsis **nssa-translator**
 no nssa-translator

Defaults None

Defaults Translation is enabled.

Command Modes OSPF VRF router configuration mode

Description Use this command to enable or disable 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 Enter **no nssa-translator** to disable NSSA Type 7-to-Type 5 translation.

Examples To disable NSAA Type 7-to-Type 5 LSA translation:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# no nssa-translator
```

See Also None

nsx-controller client-cert

Generates or deletes a self-signed certificate for the VXLAN gateway.

Synopsis **nsx-controller client-cert {generate | delete}**

Operands **generate** Generates a self-signed certificate for the VXLAN gateway.
 delete Deletes the certificate.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to generate or delete a self-signed certificate for the VXLAN gateway.

Usage Guidelines This command is supported in logical chassis cluster mode only.

Examples To generate a self-signed certificate for the VXLAN gateway:

 switch# **nsx-controller client-cert generate**

See Also

nsx-controller name

Creates an NSX controller connection profile or enters NSX controller configuration mode.

Synopsis **nsx-controller** *name*
 no nsx-controller *name*

Operands *name* Specifies a name for the NSX controller. The name is an alphanumeric, 32-character-maximum string that can also contain hyphens and underscores.

Defaults None

Command Modes Global configuration mode

Description Use this command to specify a name for a new NSX controller connection profile, or to enter NSX controller configuration mode for an existing NSX controller connection profile.

Usage Guidelines Only one NSX Controller connection profile can be configured.

This command is supported in logical chassis cluster mode only.

Use the **no** form of the command to delete an NSX controller connection profile. All active connections are closed, and all tunnels related to this NSX controller are deleted.

By default, a connection profile is inactive. To activate a profile, run the **activate** command in NSX controller configuration mode.

Examples To create an NSX controller profile named *profile1*:

```
switch# configure
switch(config)# nsx-controller profile1
```

See Also

nsx-controller name reconnect

Reconnects the NSX controller.

Synopsis `nsx-controller name name reconnect`

Operands *name* Specifies the name for the NSX controller. The name is an alphanumeric, 32-character-maximum string that can also contain hyphens and underscores.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to reinitiate a connection to the specified NSX controller if the connection was broken. If the connection is already active, this command has no effect.

Usage Guidelines This command is available only for a switch that is in logical chassis cluster mode.
The specified NSX controller connection profile name must already exist.

Examples To reconnect an NSX controller named *nsx1*:

```
sw0# nsx-controller name nsx1 reconnect
```

See Also

ntp authentication-key

Creates an authentication key to associate with the NTP server.

Synopsis **ntp authentication-key** *key-id* **md5** *md5-string*
no ntp authentication-key *key-id*

Operands *key-id* Specifies an ID for an authentication key. The range is from 1 through 65535.

md5 *md5-string* Specifies a string for the MD5 message-digest algorithm. The string can be a maximum of 15 alphanumeric characters.

Defaults None

Command Modes Global configuration mode

Description Adds an NTP authentication key (made up of a ID and an MD5 string) to a list of authentication keys in the database.

Usage Guidelines The maximum number of configurable NTP authentication keys is five. You cannot configure a duplicate key ID with a different key string. Use the **no ntp authentication-key** *key-id* command to remove the specified authentication key.

Examples To create an authentication key with an ID of 33 and an MD5 string called *check*:

```
switch# configure  
switch(config)# ntp authentication-key 33 md5 check
```

See Also **ntp server**

ntp server

Specifies or adds an NTP server IP address and associates an authentication key to the server.

Synopsis **ntp server** *ip-address* [**key** *key-id*]

no ntp server *ip-address* [**key** *key-id*]

Operands *ip-address* Specifies the NTP server IPv4 IP address (dot-decimal notation) or the IPv6 IP address (hexadecimal colon-separated notation).

key *key-id* Associates a key from the key list to the specified server. The range for a key ID is from 1 through 65535.

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, Also, use this command to associate an existing authentication key with an NTP server IP address.

Usage Guidelines The maximum number of NTP servers allowed is five.

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

Use the **no ntp server** *ip-address* command to remove the specified NTP server IP address. Removing the current active NTP server resets the NTPstatus to “LOCL” until a new, active server is selected.

Use the **no ntp server** *ip-address* **key** *key-id* command to remove the key from the specified NTP IP address.

Examples To associate a configured key ID of 15 to an NTP server:

```
switch(config)# ntp server 192.168.10.1 key 15
```

To remove an NTP server from the current list of NTP servers:

```
switch(config)# no ntp server 192.168.10.1
```

See Also **show ntp status, show clock,ntp authentication-key**

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 [<i>netmask</i>] [up]	Configures the active network interface.
ls [-al] [<i>path</i>]	Lists files and directories on the switch.
mkdir <i>dir</i>	Creates a directory.
mv [<i>i</i>] <i>file1 file2</i>	Renames a file or directory.
rm [-rf] <i>file</i>	Removes a file or directory.
rmdir	Removes a directory.
tcpdump	Analyzes network traffic. The following parameters are supported with the Network OS implementation. Refer to the Linux documentation for more information on how to use this command. Parameters: -AbdDefIKILnNOpqRStuUvxX • -B <i>buffer_size</i> • -c <i>count</i> • -C <i>file_size</i> • -G <i>rotate_seconds</i> • -F <i>file</i> • -i <i>interface</i> • -m <i>module</i> • -M <i>secret</i> • -r <i>file</i> • -s <i>snaplen</i> • -T <i>type</i> • -w <i>file</i> • -W <i>filecount</i> • -E <i>spi@ipaddr</i> • -y <i>datalinktype</i> • -z <i>postrotate-command</i> • -Z <i>user [expression]</i>

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

overlay-gateway (for VXLAN)

Creates an overlay gateway instance to function as a VXLAN gateway.

Synopsis **overlay-gateway** *name*
 no overlay-gateway *name*

Operands *name* Specifies a name for the gateway. Only one gateway instance can be configured. The name is an alphanumeric, 32-character-maximum string that can also contain hyphens and underscores.

Defaults None

Command Modes Global configuration mode

Description Use this command to create a VXLAN overlay gateway instance of the given name. An overlay network is a virtual network that is built on top of existing network Layer 2 and Layer 3 technologies.

The objectives of setting up a gateway are:

- Configuring the source IP address
- Configuring the VLAN
- Configuring MACs to export to the VXLAN domain
- Enabling statistics for interested VLAN domains
- Enabling SPAN.

One you create the gateway instance, you enter VXLAN Gateway Configuration mode, where you can configure other properties for this gateway.

Usage Guidelines Only one gateway instance can be configured.

This command is allowed for a switch that is in logical chassis cluster mode only.

Use the **no** form of the command to delete the gateway instance from the cluster. All tunnels for this gateway are also deleted.

By default, an overlay gateway instance is inactive. To activate an instance, first configure its other properties (such as which Rbridges it attaches to), then run the **activate** command .

Examples To create a VXLAN overlay gateway instance named *gateway1*:

```
switch# configure
switch(config)# overlay-gateway gateway1
```

See Also

password-attributes

Configures the 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. Valid values range from 8 through 32 characters. The default is 8 characters.

max-retry *maxretry* Specifies the number of failed password logins permitted before a user is locked out. The lockout threshold range is 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 0, 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 0, 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 range is 0 through 32 characters. The default is 0.

special-char *numsplchars* Specifies the number of punctuation characters that must occur in the password. All printable, nonalphanumeric punctuation characters, except colon (:) are allowed. The default value is 0.

Defaults The default for *minlen* is 8. All other defaults are 0.

Command Modes Global configuration mode

Description Use this command to configure global password attributes.

Usage Guidelines Enter **no password-attributes** *parameters* to set the specified password attributes to their 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
```

2 password-attributes

```
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

password-attributes admin-lockout enable

Enables the lockout policy for admin role accounts.

Synopsis **password-attributes admin-lockout enable**
 no password-attributes admin-lockout enable

Operand None

Defaults None

Command Modes Global configuration mode

Description This command enables the lockout policy for admin role accounts. Lockout policy locks admin role accounts when the user exceeds the configured number of maximum failed login attempts.

In fabric cluster mode, when the **password-attributes admin-lockout enable** command is run on one switch of the cluster, it results in the configuration being applied to all switches of the cluster.

Usage Guidelines The **no password-attributes admin-lockout enable** command disables lockout policy for admin role accounts.

Examples None

See Also None

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 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 RBridge in the Brocade VCS Fabric cluster.

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 RBridges.

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

This functionality detects Layer 2 loops only.

Enter **no pdu-rx-limit** to reset the limit to its default value.

Examples 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 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 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.

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.

Enter **no permit** to remove a rule from the MAC ACL.

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
```

2 permit (extended ACLs)

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 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.

Usage Guidelines Enter **no permit** *MAC_ADDRESS* to remove the rule affecting that address from the MAC ACL.
 Enter **no permit any** to remove all rules from the MAC ACL.

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(config-macl-std)# permit 0022.3333.4444 count
```

To delete a rule from a MAC standard ACL:

```
switch(config-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)**

pg

Creates an N_Port group in Access Gateway mode.

Synopsis **pg** *pgid*
 no pg *pgid*

Operands *pgid* Port group identifier.

Defaults None

Command Modes Access Gateway (AG) configuration

Description Use this command to configure a port group with a unique ID (*pgid*). Once configured, you can access the port group in Port Grouping configuration mode to perform configuration tasks, such as adding and removing N_Ports, enabling port group modes, and renaming the group.

Usage Guidelines You must be in Access Gateway (AG) mode to use this command. The *pgid* cannot exceed 64 characters.

Examples The following command creates port group 1 and enables Port Grouping configuration mode for the port group.

```
sw0(config-rbridge-id-3-ag)# pg 1  
sw0(config-rbridge-id-3-ag-pg-1)#
```

The following command removes port group 1.

```
sw0(config-rbridge-id-3-ag)# no pg 1
```

See Also **show ag pg**

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**] [**vrf** *vrf-name*]

Operands

<i>dest-IPv4_addr</i>	Specifies the IPv4 address of the destination device. This parameter is valid only with the ping command.
ipv6 <i>dest-ipv6-addr</i>	Specifies the IPv6 address of the destination device. This parameter is valid only with the ping command.
<i>host-name</i>	Destination host name.
count <i>number</i>	Specifies the number of transmissions (pings). The range is 1 through 655350.
timeout <i>seconds</i>	Specifies the time (in seconds) to wait for a response. The range is 1 through 60.
datagram-size <i>bytes</i>	Specifies the datagram-size (also known as the maximum transmission unit, or MTU) in bytes. The range is 36 through 9100 bytes.
quiet	Prints only the first and last line of the command output.
numeric	Do not lookup hostnames.
vrf <i>vrf-name</i>	When VRF is enabled, ping is available as a debugging tool.

Defaults The default for **count** is 1. The default for **timeout** is 1. The default for **datagram-size** is 56.

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 ---
```

2 ping

```
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 datagram 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 cir

Mandatory command for configuring the committed information rate for a class-map.

Synopsis **police cir** *cir-rate*
no police cir

Operands *cir-rate* Committed information rate. Valid values range from 40000 through 40000000000 bps in multiples of 40000.

Defaults None

Command Modes Policy-map class configuration mode

Description This command sets the committed information rate for a class-map.

Usage Guidelines When you are in config-policy-map-class mode launching the **police cir** *cir-rate* command places the system in config-policy-map-class-police mode for the configured class-map. At this point, you can add or remove additional policing parameters for the class-map.

Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples This example configures a class-map called “default” within a policy-map.

```
switch# configure terminal
switch(config)# policy-map policymap1
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch(config-policymap-class-police)#
```

See Also **cbs**, **conform-set-dscp**, **conform-set-prec**, **conform-set-tc**, **ebs**, **eir**, **exceed-set-dscp**, **exceed-set-prec**, **exceed-set-tc**, **police-priority-map**, **policy-map**, **qos cos**, **service-policy**, **set-priority**

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 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.

Enter **conform** *CoS values* or **exceed** *CoS values* while in config-policepmap 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.

Enter **no police-priority-map** *name* while in global configuration mode to remove the police-priority-map.

Enter **no conform** | **exceed** *CoS values* while in config-policepmap mode to remove CoS remapping.

NOTE

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

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 <i>policy-map name</i> no policy-map <i>policy-map name</i>
Operands	<i>policy-map name</i> Name of police policy-map
Defaults	No policy-map is created.
Command Modes	Global configuration 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 the description of the class command.)
Usage Guidelines	This command creates a Policer policy-map to apply Policer and QoS attributes to a particular interface. Each policy-map can contain up to 32 class-maps. The class-map can be associated with specific policing and QoS parameters. Maximum number of policy-map creations are 128 Associate the policy-map to the interface for inbound or outbound direction with the service-policy command. Enter no policy-map <i>name</i> while in global configuration mode to remove the policy-map. NOTE This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.
Examples	To create a policy-map and place system into config-policymap mode so that you can add a class-map: <pre>switch(config)# policy-map policymap1 switch(config-policymap)#</pre> To remove the policy-map while in global configuration mode: <pre>switch(config)# no policy-map policymap1</pre>
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 Path-cost is standard.

Command Modes Protocol Spanning Tree configuration mode

Description Use this command to set the path-cost behavior for the port-channel.

Usage Guidelines If xSTP is enabled over VCS, this command must be executed on all RBridges.

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-group

Enables port-group configuration mode for VDX 8770 Switch 27x40 GbE line cards. The mode is a prerequisite reserved for configuring Performance and Density operating modes on these line cards.

Synopsis `port-group rbridge-id/slot/port-group-id`

Operands

<code>rbridge-id</code>	A unique identifier for the switch. Values are from 1 through 239. This is not valid in standalone mode.
<code>slot</code>	Specifies a valid slot number.
<code>port-group-id</code>	A port group number (1-9) specific to the Brocade VDX 8770 switch 27x40 GbE line card.

Defaults None.

Command Modes Hardware configuration mode

Description Use this command to enter port-group configuration mode for a port group specific to a 27 x40 GbE line card. When you launch the **port-group** command, the system is placed in configuration mode for the port group. At this point, you can configure Performance or Density operating modes for the port group.

Usage Guidelines Port groups on the 27x40 GbE line card are sequentially numbered starting with 1 for ports 1-3 and ending with 9 for ports 25-27. Refer to the *Brocade 8770-4 Hardware Reference Manual* or *8770-8 Hardware Reference Manual* "Overview" chapter for more information on these port groups and configuring operating modes for this line card.

NOTE

This command is only supported on 27x40 GbE line cards installed on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples To enable port-group configuration mode for port group 9 on a line card located in slot 3 on a switch with RBridge ID 1:

```
switch(config-hardware)# port-group 1/3/9
switch(config-port-group-1/3/9)
```

See Also [hardware, port-group, mode \(27x40 GbE line card\)](#)

port-profile (global configuration mode)

Creates a new Automatic Migration of Port Profiles (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 Use this command to create a new AMPP port-profile in the fabric with the specified name and shift to the port-profile mode. If the port-profile name already exists, then the switch enters 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 submodes 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 Enter **no port-profile** *profile-name* to de-activate the port-profile.

Examples None

See Also None

port-profile (port-profile-domain configuration mode)

Adds an Automatic Migration of Port Profiles (AMPP) port-profile into a specific domain in a Virtual Fabrics context.

Synopsis **port-profile** *port-profile-name*
 no port-profile *port-profile-name*

Operands *port-profile-name* A fabric-wide unique name of a port-profile. Range is from 1 through 128 ASCII characters.

Defaults None

Command Modes Port-profile-domain configuration mode

Description Use this command to add/remove a port-profile to/from a domain in a Virtual Fabrics context,

Usage Guidelines The user must first issue the **port-profile-domain** command to enter port-profile-domain configuration mode.

In a Virtual Fabrics context, use the **port-profile-port** command to associate a profiled port to a single port-profile or a port-profile domain.

Examples Creating a port-profile in global configuration mode:

```
switch(config)# port-profile PP_Tenant_A
```

Creating a VLAN profile and enabling 802.1Q VLAN access on a trunk:

```
switch(config-port-profile-PP_Tenant_A)# vlan-profile  
switch(config-vlan-profile)# switchport mode trunk allow vlan add 10
```

In a Virtual Fabrics context, creating extended VLAN profiles (VLAN IDs > 4095) to include service or transport VFs and C-TAGs.:

```
switch(config)# port-profile PP_Tenant_B  
switch(config-vlan-profile)# switchport mode trunk allow vlan add 5000 ctag 20  
switch(config-vlan-profile)# switchport mode trunk allow vlan add 6000 ctag 30
```

In a Virtual Fabrics context, adding port-profiles to a port-profile domain.

```
switch(config)# port-profile-domain vCenter1  
switch(configport-profile-domain-vCenter1)# port-profile PP_Tenant_A  
switch(configport-profile-domain-vCenter1)# port-profile PP_Tenant_B
```

See Also **port-profile-domain, vlan-profile (AMPP)**

port-profile-domain

Creates an Automatic Migration of Port Profiles (AMPP) port-profile domain that contains all of the port-profiles that can be applied to a profiled port in a Virtual Fabrics context.

Synopsis **port-profile-domain** *port-profile-domain-name*
no port-profile-domain *port-profile-domain-name*

Operands *port-profile-domain-name*
 A fabric-wide unique name of a port-profile domain. The range is from 1 through 128 ASCII characters.

Defaults None

Command Modes Global configuration mode

Description Use this command to create an AMPP port-profile domain that contains all of the port-profiles that can be applied to a profiled port in a Virtual Fabrics context.

Usage Guidelines Within this domain, a service or transport VF (VLAN ID > 4095) must not have overlapping 802.1Q classification tags.

Enter **no port-profile-domain** *port-profile-domain-name* to delete a port-profile domain.

Use the **port-profile-port** command to associate a profiled port to a port-profile domain.

Examples Creating a port-profile domain:

```
switch(config)# port-profile-domain my_PP_domain
```

Adding profiles to the above domain:

```
switch(config-port-profile-domain-my_PP_domain)# port-profile my_PP_domain_2  
switch(config-port-profile-domain-my_PP_domain)# port-profile my_PP_domain_3
```

See Also **port-profile** (global configuration mode), **vlan-profile** (AMPP)

port-profile-port

	Activates the Automatic Migration of Port Profiles (AMPP) port-profile configuration mode on a port.
Synopsis	port-profile-port [domain <i>port-profile-domain-name</i>] no port-profile-port [domain <i>port-profile-domain-name</i>]
Operands	domain Selects a port-profile domain. <i>port-profile-domain-name</i> Name of a port-profile domain.
Defaults	When the domain keyword is not used, the port-profiles in the default profile domain are used.
Command Modes	Interface subtype configuration mode
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 facilitate comparing port-profiles within or across fabrics for robust VM migration. In a Virtual Fabrics context, use this command with the domain keyword to associate a profiled port to a port-profile domain. The result is that all service or transport VFs (VLAN ID > 4095) so specified are configured on the port.
Usage Guidelines	To apply multiple port-profiles to the interface, create and add the profiles to the default domain or to a user-created domain and apply it to the interface. • If multiple port-profiles are added to the default domain, use the port-profile-port command without the domain keyword. • If multiple port-profiles are added to a user-created domain (for example, domain_d1), use the domain keyword as in the following example: port-profile-port domain domain_d1 When the port-profile-port command is issued without the domain keyword, the domain referred to is identified by “default.” The default domain is automatically created by the system during a firmware upgrade from releases prior to NOS release 4.1.0. When the upgrade is complete, this domain contains the set of port-profiles that were created before the upgrade. Enter the no port-profile-port and no shutdown commands to remove the complete AMPP configuration from the selected port. Enter no port-profile-port domain port-profile-domain-name to dissociate the profiled port from the port-profile domain. NOTE In VF-enabled mode only, the user can manage port-profiles in a default domain as in any other domain.
Examples	The following examples illustrate activating AMPP port-profile configuration mode on a specific 10-gigabit Ethernet interface port. To associate the default port-profile domain to an interface: <pre>switch(config)# interface tengigabitethernet 178/0/9 switch(conf-if-te-178/0/9)# port-profile-port</pre>

2 port-profile-port

To associate a profiled port with a user-specified port-profile domain:

```
switch(config)# interface tengigabitethernet 178/0/9  
switch(conf-if-te-178/0/9)# port-profile-port domain vDC1
```

See Also interface, shutdown, port-profile (global configuration mode), port-profile-domain

port-shape

Specifies the shaping rate for a port.

Synopsis **port-shape** *speed*

Operands *speed* The speed for the port-shape rate in Kbps. The range of valid values is from 28000 to the top speed on the interface.

Defaults None

Command Modes Policymap configuration mode

Description Use this command to specify the shaping rate for a port. You can use this command to smooth out the traffic egressing an interface.

Usage Guidelines This command is allowed only for the Egress direction.
This command can only be configured in for the **class class-default** command.
This command is mutually exclusive of the **scheduler** and **police** commands.

Examples Typical command example:

switch(config)#**policy-map** *mutation*
switch(config-policy-map)#**class** *class-default*
switch(config-policyclass)# **port-shape** 30000

See Also **class**, **policy-map**

power-off

Deactivates a line card or Switch Fabric Module (SFM).

Synopsis **power-off** {**linecard** | **sfm**} {*m4_value* | *m8_value*}

Operands	linecard	Selects a line card to deactivate.
	sfm	Selects an SFM to deactivate.
	<i>m4_value</i>	The slot number. If you are using a Brocade VDX 8770-4 switch, the range of values is from 1 through 3.
	<i>m8_value</i>	The slot number. If you are using a Brocade VDX 8770-8 switch, the range of values is from 1 through 6.

Defaults None

Command Modes Global configuration mode

Description This command deactivates a line card or Switch Fabric Module (SFM) on a switch.

Usage Guidelines None

Examples None

See Also None

power-off linecard

Powers off a line card.

Synopsis **power-off linecard** *slot_number*

Operands *slot_number* Specifies the slot number to be powered-off. Line card slots are 1 through 4 on a Brocade VDX 8770-4 and 1 through 8 on a Brocade VDX 8770-8.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to power off a line card. A line card must be powered off before you can change the slot configuration.

Usage Guidelines None

Examples To power off a line card in slot 4:

 switch# **power-off linecard 4**

See Also linecard, power-on linecard, show running-config rbridge-id linecard

power-on

Activates a line card or Switch Fabric Module (SFM).

Synopsis **power-on** {**linecard** | **sfm**} {*m4_value* | *m8_value*}

Operands	linecard	Selects a line card to activate
	sfm	Selects an SFM to activate.
	<i>m4_value</i>	The slot number. If you are using a Brocade VDX 8770-4 switch, the range of values is from 1 through 3.
	<i>m8_value</i>	The slot number. If you are using a Brocade VDX 8770-8 switch, the range of values is from 1 through 6.

Defaults None

Command Modes Global configuration mode

Description This command activates a line card or Switch Fabric Module (SFM) on a switch.

Usage Guidelines None

Examples None

See Also None

power-on linecard

Powers on a line card.

Synopsis	power-on linecard <i>slot_number</i>	
Operands	<i>slot_number</i>	Specifies the slot number to be powered-on. Line card slots are 1 through 4 on a Brocade VDX 8770-4 and 1 through 8 on a Brocade VDX 8770-8.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to power on a line card.	
Usage Guidelines	None	
Examples	To power on a line card 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. Valid values range from 1 through 100.

Defaults The default is 1.

Command Modes CEE map configuration mode

Description Use this command to set the precedence of the CEE map.

Usage Guidelines None

Examples To set the precedence to 1:

 switch(config-cee-map-default)# **precedence 1**

See Also None

preempt-mode

Turns on preempt mode for a VRRP router session.

Synopsis **preempt-mode**
 no preempt-mode

Operands None

Defaults Enabled for VRRP; Disabled for VRRP-E.

Command Modes Virtual-router-group configuration mode

Description Use this command to enable or disable preempt mode for a virtual router session. 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.

 For VRRP-E, the interface must be **ve**.

 Enter **no preempt-mode** to turn off preempt mode.

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(config-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 VRRP router group.

Synopsis *priority range*

Operands *range* The priority of a physical router in a virtual router group. Higher numbers have priority over lower numbers. Valid values range from 1 to 254.

Defaults The default is 1.

Command Modes Virtual-router-group configuration mode

Description Use this command to set the priority of a physical router in a VRRP 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(config-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-extended
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. Valid values range 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. Valid values range from 1 through 100.

pfc Enables the Priority-based Flow Control (PFC) for each priority that gets mapped to the priority group.

on Enables PFC.

off Disables PFC.

Defaults There is no default value for the weight. PFC is disabled.

Command Modes CEE map configuration mode

Description Use this command to set the bandwidth for each priority group.

Enter **priority-group-table** 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 from 0 through 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 a PGID of 15.1 is higher priority than a PGID of 15.2.

Enter **no priority-group-table** *pgid* 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. The following lists the bandwidth allocation to user priority groups.

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 predefined in the switch.

Examples To define the CEE map and configure the bandwidth with the priority group, use the values in Table .

```
switch(config)# cee-map test
```

2 priority-group-table

```
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 The priority-tag is disabled for all supported interfaces.

Command Modes Interface subtype configuration mode

Description Use this command to toggle the priority-tagging support on a specific interface. This command is the only method for toggling priority-tagging.

Usage Guidelines Enter **no priority-tag** to disable priority-tagging support.

Example To enable priority-tagging support on a specific 10-gigabit Ethernet interface:

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

See Also **interface, cee-map (FCoE)**

private-vlan

Configures a VLAN as a private VLAN (PVLAN).

Synopsis **private-vlan** [**isolated** | **community** | **primary**]
 no private-vlan [**isolated** | **community** | **primary**]

Operands **isolated** The PVLAN is configured as an Isolated VLAN.
 community The PVLAN is configured as a Community VLAN.
 primary The PVLAN is configured as a Primary VLAN.

Defaults None

Command Modes VLAN interface configuration mode

Description Use this command to configure a VLAN as a private VLAN (PVLAN).

Usage Guidelines None

Examples None

See Also **private-vlan association**

private-vlan association

Associates a secondary VLAN to a primary VLAN.

Synopsis **private-vlan association** [**add** *vlan_id* | **remove** *vlan_id*]
 no private-vlan association [**add** *vlan_id* | **remove** *vlan_id*]

Operands **add** *vlan_id* Adds the association.
 remove *vlan_id* Removes the association.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to associates a secondary VLAN to a primary 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also **private-vlan**

profile

Creates an LLDP profile.

Synopsis **profile** *name*
 no profile *name*

Operands *name* Assigns a name to the profile. The name must be between 1 and 63 ASCII characters in length.

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.

Enter **no profile** *name* to remove the named profile.

Examples To create a profile named test:

 switch(conf-lddp) # **profile test**

 To delete a profile named test:

 switch(conf-lddp) # **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 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 **unhide fips** with the password “**fibranne**” to make the command available.

ATTENTION

Use this command only when preparing a switch for FIPS compliance.



CAUTION

Once Boot PROM access is disabled, you cannot re-enable it.

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 Use this command to enable or disable protect mode. In the Blade Center Chassis environment, the Advanced 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 Enter **no protect-mode enable** to disable this command.

Examples None

See Also None

protocol edge-loop-detection

Sets the edge-loop detection (ELD) 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.

Usage Guidelines Enter **no protocol lldp** to restore the default settings.

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 | rpvt}**
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+).
rpvt Specifies Rapid Per-VLAN Spanning Tree Protocol Plus (R-PVST+).

Defaults 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.

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.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Brocade Network OS v4.1.0 supports PVST+ and R-PVST+ only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Enter **no protocol spanning-tree** to delete the context and all the configurations defined within the context or protocol for the interface.

Examples To enable the Spanning Tree Protocol:

```
switch(config)# protocol spanning-tree stp
```

See Also **show spanning-tree**

protocol udd

Enables and/or enters unidirectional link detection (UDLD) protocol configuration mode.

Synopsis **protocol udd**
 no protocol udd

Operands None

Defaults This protocol is disabled by default.

Command Modes Global configuration mode

Description UDLD detects and blocks a physical link that becomes unidirectional. A unidirectional link can cause traffic in a network to loop endlessly. When the link becomes bidirectional again, UDLD unblocks the link.

Usage Guidelines This protocol applies only to physical ports. In addition to running this command, you must also enable each desired port for UDLD in interface subconfiguration mode.

Use the **no protocol udd** command to disable the UDLD protocol and revert all UDLD configuration to defaults.

Examples To enable the unidirectional link detection (UDLD) protocol:

```
switch# configure  
switch(config)# protocol udd
```

See Also **hello (UDLD), udd enable, shutdown (UDLD)**

protocol vrrp

Globally enables VRRP (and VRRP-E on some platforms).

Synopsis **protocol vrrp**
 no protocol vrrp

Operands None

Defaults Disabled

Command Modes RBridge ID configuration mode (For a switch in standalone mode, this command is available in global configuration mode.)

Description Enables both the VRRP and VRRP-Extended protocols on the Brocade VDX 8770, 6710, 6720, and 6730, and enables VRRP on the Brocade VDX 6740.

Usage Guidelines The **no protocol vrrp** command globally disables only VRRP but not VRRP-E.

Examples To enable VRRP and VRRP-E on the VDX 8770:

```
switch# configure  
switch(config)# rbridge-id 101  
switch(config-rbridge-id-101)# protocol vrrp
```

See Also **protocol vrrp-extended**

protocol vrrp-extended

Globally enables VRRP-Extended.

Synopsis **protocol vrrp-extended**
 no protocol vrrp-extended

Operands None

Defaults Disabled

Command Modes RBridge ID configuration mode (For a switch in standalone mode, this command is available in global configuration mode.)

Description Enables the VRRP-Extended protocol.

Usage Guidelines The **no protocol vrrp-extended** command globally disables VRRP-Extended.

Examples To enable VRRP-Extended:

```
switch# configure  
switch (config)# rbridge-id 101  
switch(config-rbridge-id-101)# protocol vrrp-extended
```

See Also **protocol vrrp**

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. Valid values range from 0 through 7.

Defaults The default is 0.

Command Modes Interface subtype configuration mode

Description Use this command to specify the interface Default CoS value. When Interface ingress QoS Trust is in the un-trusted 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 nonpriority 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.

Enter **no qos cos** to return the CoS value to the default.

Examples To set the CoS value to 2 on a specific 40-gigabit Ethernet 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 No explicit CoS-to-CoS mutation QoS map is applied; the inbound CoS equals the outbound CoS.

Command Modes Interface subtype configuration mode

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.
Enter **no qos cos-mutation** to remove the CoS-to-CoS mutation map.

Examples To activate a CoS-to-CoS mutation QoS map named *test* on a specific 40-gigabit Ethernet 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 No explicit CoS-to-Traffic Class QoS map is applied; the implicit behavior is to match the IEEE 802.1Q recommendations for systems supporting 8 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.
 Enter **no qos cos-traffic-class** to remove the CoS-to-Traffic Class mapping.

Examples To apply a CoS-to-Traffic Class QoS map named *test* to a specific 10-gigabit Ethernet 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 Enter **no qos dscp-cos** 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 subtype configuration mode

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 Enter **no qos dscp-mutation** 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 subtype configuration mode

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 Enter **no qos dscp-traffic-class** 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 **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 **no qos dscp-traffic-class** 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 **rx**

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 sub ~~type~~ configuration mode (~~fo, gi, port-channel, te~~)															
Description	Use this command to configure and activate QoS flow control.															
	When a 1-Gbps 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 below.															
	Pause negotiation results <table><tr><th>Advertised LOCAL cfg</th><th>Advertised REMOTE cfg</th><th>Negotiated result</th></tr><tr><td>Rx=off Tx=on</td><td>Rx=on Tx=on</td><td>asymmetrical: LOCAL Tx=on --> pause --> REMOTE Rx=on</td></tr><tr><td>Rx=on Tx=on</td><td>Rx=off Tx=on</td><td>asymmetrical: LOCAL Rx=on <-- pause <-- REMOTE Tx=on</td></tr><tr><td>Rx=on Tx=n/a</td><td>Rx=on Tx=n/a</td><td>symmetrical : LOCAL Tx/Rx=on <-- pause --> REMOTE Tx/Rx=on</td></tr><tr><td>Rx=n/a Tx=n/a</td><td>Rx=off Tx=off</td><td>disable pause both sides</td></tr></table>		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
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	Enter no qos flowcontrol to deactivate flow control on a specific interface.															
Examples	To activate both the transmitting and receiving portions of flow control on a specific 40-gigabit Ethernet interface:															
	<pre>switch(config)# interface fortygigabitethernet 1/3/1 switch(conf-fo-1/3/1)# qos flowcontrol tx on rx on</pre>															
	To deactivate flow control on a specific port-channel interface:															
	<pre>switch(config)# interface port-channel 33 switch(config-port-channel-33)# no qos flowcontrol</pre>															
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 subtype configuration mode

Description Use this command to activate and configure flow control for a Class of Service.

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.
- Only affects per-interface pause behavior. To use flow control in Brocade VCS Fabric mode, use the CEE map configuration.

Enter **no qos flowcontrol pfc** *cos_value* 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 40-gigabit Ethernet interface:

```
switch(config)# interface fortygigabitethernet 1/3/1
switch(config-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 No CoS-to-CoS mutation QoS maps are 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.

Usage Guidelines Enter **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 having inbound CoS 4 mapped to outbound CoS 5 and inbound CoS 5 mapped to outbound CoS 4; but 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 No CoS-to-Traffic Class QoS maps are 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.

Usage Guidelines Enter **no qos map cos-traffic-class** *name* to delete the CoS-to-Traffic Class QoS map specified by *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 8 Traffic Classes.

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 qos 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 create and remove QoS dscp-cos maps, which remap the incoming DSCP values of the ingress packet to egress CoS 802.1P values.

Usage Guidelines When you enter **qos map dscp-cos**, 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.

Enter **qos dscp-cos** *name* while in configuration mode for a specific interface to apply the DSCP-CoS map to that interface.

Enter **no qos dscp-cos** *name* while in the interface configuration mode to remove the map from the interface.

Enter **no map dscp-cos** *name* while in global configuration mode to remove the DSCP-CoS map.

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 create a QoS dscp-mutation map. Use this command to remap the incoming DSCP values of the ingress packet to an egress DSCP value.

Usage Guidelines Enter **qos dscp-mutation** *name* while in configuration mode for a specific interface to apply the dscp-mutation map to that interface. When you enter **qos map dscp-mutation**, 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.

Enter **no qos dscp-mutation** *name* while in interface configuration mode to remove the map from that interface.

Enter **no map dscp-mutation** *name* while in global configuration mode to remove the dscp-mutation map.

NOTE

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

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
```

2 qos map dscp-mutation

NOTE

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

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 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 create a QoS DSCP-Traffic-Class map. Use this command to remap the incoming DSCP values of the ingress packet to a Traffic Class.

Usage Guidelines Enter **qos dscp-traffic-class** *name* while in configuration mode for a specific interface to apply the QoS DSCP-Traffic-Class map to that interface. When you enter **qos map dscp-traffic-class**, 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.

Enter **no qos dscp-traffic-class** *name* while in the interface mode to remove the map from that interface.

Enter **no map dscp-mutation** *name* to remove the map while in global configuration 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-IDvalue*

Operands

<i>profile-ID value</i>	Valid values range from 1 through 384.
<i>percentage</i>	0 through 100 percent.
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 Use this command to create a Random Early Discard (RED) profile and provides a minimum threshold, maximum threshold, and drop-probability for egress traffic flow.

Usage Guidelines Enter **qos random-detect cos** command while in configuration mode for a specific interface to map the profile to a CoS priority for a port.

Enter **no qos random-detect cos** command while in the interface mode to remove the profile from the interface. You must remove the profile from interface before you can remove the profile itself.

Enter **no qos red-profile** *profile-ID* to remove the profile while in global configuration mode.

NOTE

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

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 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 subtype configuration mode

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.

Enter **no qos trust cos** to return to the default.

Examples To set the interface QoS to the CoS trust mode for a specific 10-gigabit Ethernet 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 subtype configuration mode																		
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 following lists the default mapping of DSCP values to user priority. Default DSCP priority mapping <table><tr><th>DSCP Values</th><th>User Priority</th></tr><tr><td>0-7</td><td>0</td></tr><tr><td>8-15</td><td>1</td></tr><tr><td>16-23</td><td>2</td></tr><tr><td>24-31</td><td>3</td></tr><tr><td>32-39</td><td>4</td></tr><tr><td>40-47</td><td>5</td></tr><tr><td>48-55</td><td>6</td></tr><tr><td>56-63</td><td>7</td></tr></table>	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
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. Enter no qos trust dscp to return to the default.																		
Examples	To set the interface QoS to DCSP trust mode on a specific 10-gigabit Ethernet interface: <pre>switch(config)# interface tengigabitethernet 178/0/9 switch(conf-if-te-178/0/9)# qos trust dscp</pre> To return the interface QoS to the default value or to the untrusted state: <pre>switch(config)# interface tengigabitethernet 178/0/9 switch(conf-if-te-178/0/9)# no qos trust dscp</pre> NOTE This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.																		
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.
	<i>mTC0_WEIGHT</i>	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. Valid values range from 0 through 100.
	<i>mTC1_WEIGHT</i>	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. Valid values range from 0 through 100.
	<i>mTC2_WEIGHT</i>	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. Valid values range from 0 through 100.
	<i>mTC3_WEIGHT</i>	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. Valid values range from 0 through 100.
	<i>mTC4_WEIGHT</i>	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. Valid values range from 0 through 100.
	<i>mTC5_WEIGHT</i>	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. Valid values range from 0 through 100.
	<i>mTC6_WEIGHT</i>	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. Valid values range from 0 through 100.
	<i>mTC7_WEIGHT</i>	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. Valid values range 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.

Usage Guidelines Enter **no qos queue multicast scheduler** to return the multicast Traffic Class packet expansion scheduler to the default value.

2 qos queue multicast scheduler

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.
	<i>strict-priority-number</i>	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 Classes contains Traffic Classes 7, 6, and 5. Valid values range 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.
	<i>weight0</i>	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 <i>weight0</i> value is only valid when the strict priority number is less than 8. Valid values range from 0 through 100 percent.
	<i>weight1</i>	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 <i>weight1</i> value is only valid when the strict priority number is less than 7. Valid values range from 0 through 100 percent.
	<i>weight2</i>	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 <i>weight2</i> value is only valid when the strict priority number is less than 6. Valid values range from 0 through 100 percent.
	<i>weight3</i>	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 <i>weight3</i> value is only valid when the strict priority number is less than 5. Valid values range from 0 through 100 percent.
	<i>weight4</i>	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 <i>weight4</i> value is only valid when the strict priority number is less than 4. Valid values range from 0 through 100 percent.

<i>weight5</i>	Sets the DWRR weight for Traffic Class 5 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 <i>weight5</i> value is only valid when the strict priority number is less than 3. Valid values range from 0 through 100 percent.
<i>weight6</i>	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 <i>weight6</i> value is only valid when the strict priority number is less than 2. Valid values range from 0 through 100 percent.
<i>weight7</i>	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 <i>weight7</i> value is only valid when the strict priority number is less than 1. Valid values range 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.

Enter **no qos queue scheduler** to return the Traffic Class packet scheduler to the default value.

Examples To set the Traffic Class packet scheduler for four Strict Priority Traffic Class and four 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 random-detect cos

Maps a Random Early Discard (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. Valid values range from 0 through 7.
 profile-ID *value* Random Error Detection value. Valid values range from 1 through 384.

Defaults Port CoS priority value is not mapped to the RED profile.

Command Modes Interface subtype configuration mode

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 Enter **no qos random-detect cos** *value* 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 10-gigabit Ethernet 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 previously created 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 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	<i>TDT0</i>	Defines the proportion for the first port tail drop threshold. Valid values range from 0 through 100.
	<i>TDT1</i>	Defines the proportion for the second port tail drop threshold. Valid values range from 0 through 100.
	<i>TDT2</i>	Defines the proportion for the third port tail drop threshold. Valid values range from 0 through 100.
	<i>TDT3</i>	Defines the proportion for the fourth port tail drop threshold. Valid values range from 0 through 100.
	<i>TDT4</i>	Defines the proportion for the fifth port tail drop threshold. Valid values range from 0 through 100.
	<i>TDT5</i>	Defines the proportion for the sixth port tail drop threshold. Valid values range from 0 through 100.
	<i>TDT6</i>	Defines the proportion for the seventh port tail drop threshold. Valid values range from 0 through 100.
	<i>TDT7</i>	Defines the proportion for the eighth port tail drop threshold. Valid values range from 0 through 100.

Defaults None

Command Modes Interface subconfiguration mode (gi, te).

Description Use this command to configure the port tail drop thresholds.

Every port has associated with it a total of nine 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 any priority from 0% to 100% to any threshold; however, the sum value of all eight priorities must not exceed 100%. For example, using the priorities 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.

NOTE
Brocade recommends *not* configuring cos-thresholds on an edge interface for a COS value with pause/priority flow control enabled. Doing so could create buffer-allocation issues.

Enter **no qos rcv-queue cos-threshold** 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 Ten Gigabit Ethernet 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 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). Valid values range from 6500 through 20000000 pkt/s.

burst *burst-size* Configures a cap on the maximum burst size for multicast packet expansion. Valid values range from 50 through 65535 packets.

Defaults The burst size is 4096 packets. The rate value is 3000000 pkt/s.

Command Modes Global configuration mode

Description Use this command to configure 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.

Usage Guidelines This command is not supported on VDX 8770-4 and VDX 8770-8 switches.

The *rate* parameter 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* parameter represents the maximum number of multicast packet expansion that can be performed back-to-back as a single burst in units of packets (pkt).

Enter **no qos rcv-queue multicast rate-limit** to return the multicast packet expansion rate limit to the default settings.

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	<i>mTC0</i>	Sets the Tail Drop Threshold for multicast Traffic Class 0 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.
	<i>mTC1</i>	Sets the Tail Drop Threshold for multicast Traffic Class 1 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.
	<i>mTC2</i>	Sets the Tail Drop Threshold for multicast Traffic Class 2 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.
	<i>mTC3</i>	Sets the Tail Drop Threshold for multicast Traffic Class 3 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.
	<i>mTC4</i>	Sets the Tail Drop Threshold for multicast Traffic Class 4 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.
	<i>mTC5</i>	Sets the Tail Drop Threshold for multicast Traffic Class 5 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.
	<i>mTC6</i>	Sets the Tail Drop Threshold for multicast Traffic Class 6 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.
	<i>mTC7</i>	Sets the Tail Drop Threshold for multicast Traffic Class 7 packet expansion queue in units of packets (pkt). The valid range is 0 through 16383 packets.

Defaults 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.

Usage Guidelines This command is not supported on VDX 8770-4 and VDX 8770-8 switches.

Enter **no qos rcv-queue multicast threshold** to return the multicast expansion queues to the default value.

2 qos rcv-queue multicast threshold

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 configuration mode

Description Use this command to activate the QoS profile mode for AMPP. This mode allows configuration of QoS attributes of a port-profile.

Usage Guidelines Enter **no qos-profile** 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*] [**encryption-level** *value_level*] [**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 *portnum* 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. Parameters 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 (\). For example: "**secret!key**" or **secret\!key**.

encryption-level

value_level Designates the encryption level for the shared secret key operation. This operand supports JITC certification and compliance. The range of valid values is from 0 through 7, with 0 being clear text and 7 being the most heavily encrypted. The default value is 0.

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
- **encryption-level** 0
- **key:** sharedsecret
- **protocol:** CHAP

Command Modes Global configuration mode

Description 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 **key** parameter does not support an empty string.
Enter **no radius-server** to reset to their default values.

NOTE

Before downgrading to a Network OS version that does not support the **encryption-level** keyword, set the value of this keyword to **0**. Otherwise, the firmware download will throw an error that requests this value be set to **0**.

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**

rasman

Provides instant customer access to RASLog messages decoding and documentation on the switch.

Synopsis **rasman** [[**module-description**] | [**message id** *RAS-message-id*] | [**module type** *module-name*] | [**type value** *RAS-message-type*]]

Operands **module-description** Displays the RAS module description.

message id *RAS-message-id*

 Displays the RAS message ID details.

module type *module-name*

 Displays the RAS message ID based on module. Displays all external RAS messages.

type value *RAS-message-type*

 Displays the RAS message ID based on type. Possible completions: AUDIT, DCE, FFDC, LOG, and VCS.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to access RASLog messages decoding and documentation on the switch.

Usage Guidelines Input value is case-sensitive.

Examples Example output of **rasman module-description** command:

```
sw0# rasman module-description
```

RASModule	ID	Description
KT	1	Kernel Test ID
UT	2	User Test ID
TRCE	3	Trace Subsystem (User)
KTRC	4	Trace Subsystem (Kernel)
LOG	5	RASLOG module
CDR	6	Condor ASIC driver

Example of **rasman module type AUTH**:

```
sw0# rasman module type AUTH
```

RAS Message ID	Severity	Message
AUTH-1001	INFO	%s has been successfully completed.
AUTH-1002	ERROR	%s has failed.

AUTH-1003	INFO	%s type has been successfully set t
AUTH-1004	ERROR	Failed to set %s type to %s.
AUTH-1005	ERROR	Authentication file does not exist:
AUTH-1006	WARNING	Failed to open authentication confi
AUTH-1007	ERROR	The proposed authentication protoco
AUTH-1008	ERROR	No security license, operation fail

Example of rasman type value AUDIT:

```
sw0# rasman type value AUDIT
```

RAS Message ID	Severity	Message
FCIP-1002	INFO	An IPsec/IKE policy was added
FCIP-1003	INFO	An IPsec/IKE policy was deleted
AUTH-1045	ERROR	Certificate not present in this switch
AUTH-1046	INFO	%s has been successfully completed
AUTH-1047	ERROR	%s has failed
AUTH-3001	INFO	Event: %s, Status: success, Info: %
AUTH-3002	INFO	Event: %s, Status: success, Info: %

Example of rasman type value DCE:

```
sw0# rasman type value DCE
```

RAS Message ID	Severity	Message
LACP-1001	ERROR	%s Error opening socket (%d)
LACP-1002	ERROR	%s %s
LACP-1003	INFO	Port-channel %d up in defaulted state
LACP-1004	INFO	Port-channel %d down from default
NSM-1001	INFO	Interface %s is online
NSM-1002	INFO	Interface %s is protocol down

Example of rasman type value LOG:

```
sw0# rasman type value LOG
```

RAS Message ID	Severity	Message
FCIP-1000	ERROR	%s of GE %d failed. Please retry
FCIP-1001	CRITICAL	FIPS %s failed; algo=%d type=%d slot
FCIP-1002	INFO	An IPsec/IKE policy was added

2 rasman

FCIP-1003	INFO	An IPsec/IKE policy was deleted
FCIP-1004	INFO	Tape Read Pipelining is being disabled
AUTH-1001	INFO	%s has been successfully completed
AUTH-1002	ERROR	%s has failed

Example of rasman type value VCS:

```
sw0# rasman type value VCS
RAS Message ID      Severity      Message
-----
SS-2000             INFO         Copy support started on rbridge-id
SS-2001             INFO         Copy support completed on rbridge-id
SS-2002             INFO         Copy support failed on rbridge-id %
SULB-1105           WARNING      Firmware upgrade session (%d: %s) s
SULB-1106           WARNING      Firmware upgrade session (%d: %s) c
SULB-1107           WARNING      Firmware upgrade session (%d: %s) f
```

See Also None

rate-limit-delay get netconf

Returns the rate limit delay configured for processing NETCONF Remote Procedure Calls (RPCs).

Synopsis `rate-limit-delay get netconf`

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to learn the configured minimum time in milliseconds between processing successive NETCONF RPCs. A value of 0 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`rate-limit-delay set netconf delay`

Operands	<i>delay</i>	The number of milliseconds the system waits between processing RPCs.
Defaults	The default is 0.	
Command Modes	Privileged EXEC mode	
Description	Use this command to limit the rate at which RPCs can be processed on the switch by specifying the minimum delay between processing successive RPCs. The default of 0 means that the RPC processing rate is unlimited.	
Usage Guidelines	Use this command to prevent excessive numbers of RPCs from adversely affecting switch performance.	
Examples	This example limits the processing of RPCs to a maximum of one every 50 milliseconds. <code>switch# debug internal rate-limit-delay set netconf 50</code>	
See Also	<code>rate-limit-delay get netconf</code>	

rbridge-id

Enables RBridge ID configuration mode to support VCS on individual nodes.

Synopsis **rbridge-id** *rbridge-id*
 no rbridge-id *rbridge-id*

Operands *rbridge-id* The number of an RBridge node.

Defaults None

Command Modes Global configuration mode

Description Use this command to enter RBridge ID configuration mode for fabric cluster and logical chassis cluster configuration.

Usage Guidelines



CAUTION

It is always preferable to have the RBridge ID configured on a switch. If the RBridge ID is not configured, deleting the interface IP address that matches the router ID will cause an OSPF process reset and a spike in CPU usage.

Examples Use the **rbridge-id ?** command in global configuration mode to see available nodes.
 Enter RBridge ID configuration mode and use **?** to view commands available in that mode:

```
sw0(config)# rbridge-id 154
sw0(config-rbridge-id-154)# ?
Possible completions:
  arp                      Address Resolution Protocol (ARP)
  chassis
  do                       Run an operational-mode command
  exit                    Exit from current mode
  fabric                  Allows to configure fabric related parameters
  fcsp                   FCSP configuration commands
  filter-change-update-delay Change filter change update delay timer
  help                   Provide help information
  interface              Interface configuration
  ip                     Configure Internet Protocol (IP)
  ipv6                   Configure Internet Protocol (IPv6)
  logical-chassis        Logical chassis commands
  management             The list of management interfaces.
  no                     Negate a command or set its defaults
  protocol               Protocol configuration
  pwd                    Display current mode path
  route-map              Configure a route-map instance
  router                 Configure router
  secpolicy              Security policy related configuration
  ssh                    Configure SSH Server
  switch-attributes      Switch attributes configurations
  system-monitor         Configure FRU threshold and alert setting
  telnet                 Configure Telnet Server
  threshold-monitor      Configure Class monitoring threshold and alert
```

2 rbridge-id

top
vrf

setting
Exit to top level and optionally run command
VRF configurations

See Also None

rd (route distinguisher)

Distinguishes a route for VRF.

Synopsis `rd admin-value:arbitrary-value`

Operands

<i>admin-value</i>	The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2-byte number (from 0 through 65535) or a 4-byte number (from 0 through 4294967295).
<i>arbitrary-value</i>	An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is 2 byte, or from 0 through 4294967295 if the ASN is 4 byte.

Defaults None

Command Modes VRF configuration mode

Description Use this command to distinguish a route to which the VRF belongs. The command allows the same IP address to be used in different VPNs without creating any conflicts. The Route Distinguisher parameter can be either ASN-relative or IP address-relative.

Usage Guidelines Once the Route Distinguisher is configured for a VRF it cannot be changed or deleted.
To remove the Route Distinguisher, you must delete the VRF.

Examples To configure Route Distinguisher:

```
switch# configure terminal
Entering configuration mode terminal
switch(config)# rbridge-id 53
switch(config-rbridge-id-53)# vrf red
switch(config-vrf-red)# rd 101:101
```

To remove Route Distinguisher, remove the VRF.

```
switch(config-vrf-red)# no vrf red
```

See Also `vrf`, `ip router-id`

reconnect-interval

Sets the reconnect interval between the NSX controller and the VCS fabric.

Synopsis **reconnect-interval** *interval*
 no reconnect-interval

Operands *interval* Specifies the maximum number of seconds to wait between connection attempts. Value must be in the range of 1 to 1000.

Defaults 10 seconds

Command Modes NSX Controller configuration mode

Description Use this command to set the reconnect interval for the NSX controller connection profile. If the connection is lost between the NSX and the VCS fabric, a reconnection attempt occurs at this interval.

Usage Guidelines This command is allowed for a switch that is in logical chassis cluster mode only.
 Use the **no** form of the command to revert the reconnect interval to the default value.

Examples To set the reconnect interval to 30 seconds for an NSX controller profile that you have already created (named *profile1*):

```
switch# configuration  
switch(config)# nsx-controller profile1  
switch(config-nsx-controller-profile1)# reconnect-interval 30
```

See Also

redistribute (BGP)

Configures the device to redistribute OSPF, ISIS, or RIP routes, directly connected routes, or static routes into BGP4.

Synopsis **redistribute** {**connected** | **static**} [**metric** *num*] | **route-map** *string*
no redistribute {**connected** | **static**} [**metric** *num*] | **route-map** *string*

Operands **connected** Redistributes connected routes.
 static Redistributes static routes.
 The range is from 0 through 4294967297.
 string Specifies a route map to be consulted before an OSPF route is added to the BGP4 routing table.

Defaults No value is assigned for *num*.

Command Modes BGP address-family IPv4 unicast configuration mode

Description By default, the device does not redistribute routing information between BGP4 and the IP interior gateway protocol OSPF. Use this command to configure the device to redistribute OSPF, directly connected routes, or static routes into BGP4. The routes can be filtered by means of an associated route map before they are distributed.

Usage Guidelines Use the **no** form of the command to restore the defaults.

NOTE
The **default-metric** command does not apply to the redistribution of directly connected routes into BGP4. Use a route map to change the default metric for directly connected routes.

Examples `switch(config)# rbridge-id 10`
 `switch(config-rbridge-id-10)# router bgp`
 `switch(config-bgp-router)# address-family ipv4 unicast`
 `switch(config-bgp-ipv4u)# redistribute static metric 200`

See Also **default-metric (OSPF), route-map**

redistribute (OSPF)

Configures the device to redistribute OSPF routes.

Synopsis **redistribute ospf** {**match** [**external1** | **external2** | **internal**]} [**metric** *num*] | **route-map** *string*
no redistribute ospf {**match** [**external1** | **external2** | **internal**]} [**metric** *num*] | **route-map** *string*

Operands

match	Selects the type of route to be redistributed.
external1	Redistributes OSPF external type 1 routes.
external2	Redistributes OSPF external type 2 routes.
internal	Redistributes OSPF internal routes.
<i>num</i>	A value that assigns the metric. The range is from 0 through 4294967297.
<i>string</i>	Specifies a route map to be consulted before an OSPF route is added to the BGP4 routing table.

Defaults Internal OSPF routes are distributed. No value is assigned for *num*.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to redistribute OSPF external type 1, external type 2, or internal routes.

Usage Guidelines Use the **redistribute ospf** command to redistribute all OSPF routes. Use the **no** form of the command to restore the defaults.

Examples

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# redistribute ospf match external1 metric 200
```

See Also **default-metric (OSPF)**

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 configuration mode

Description Use this command to assign a name to an MSTP region.

Usage Guidelines The *region-name* string must be between 1 and 32 ASCII characters in length, and is case-sensitive.

If MSTP is enabled over VCS, this command must be executed on all RBridge nodes

Enter **no region** to delete the region name.

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 (MM).

Synopsis **reload** [**standby** | **system**]
reload system [**rbridge-id** {*rbridge-id* | **all**}]

Operands **standby** Reboots the standby CP or MM on a dual CP/MM chassis.
system Reboots an entire chassis.
rbridge-id *rbridge-id* Reloads the designated RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to perform a “cold reboot” (power off and restart) of the CP or MM.

Usage Guidelines The **reload** operation is generally 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.

The available modes are listed below.

Available modes	
Mode	Definition
Standalone	Standalone. A node is in Standalone mode when Virtual Cluster Switching (VCS) is disabled.
FC	Fabric cluster. In FC mode, the data path for nodes is distributed, but the configuration path is not distributed. Each node maintains its own configuration database.
LC	Logical chassis cluster. In LC mode, both the data path and the configuration path are distributed.

The following summarizes the behavior of the **reload** command under a variety of conditions.

Behavior of the **reload** command

Command	HA synchronized		HA not synchronized	
	Active	Standby	Active	Standby
reload	If executed on active MM, reboots that MM ¹ .	If executed on active MM, reboots that MM.	The user is prompted to execute the reload system command.	N/A
	In FC mode, the running configuration becomes the new active configuration.			N/A
	In LC mode, the running configuration becomes the new active configuration.			N/A
reload standby	Reboots the standby MM.	Reboots the standby MM.	Reboots the standby MM.	Reboots the standby MM.
reload system	Reboots the chassis and remains the master MM.	Not allowed.	If executed on active MM, reboots the chassis and remains the master MM.	Not allowed.
	In FC mode, the startup configuration is used.		In FC mode, the startup configuration is used.	
	In LC mode, the running configuration is used.		In LC mode, the running configuration is used.	

NOTE

MM = Management module

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](#), [ha chassisreboot](#), [ha failover](#)

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 valid range is 0 through 6.

Defaults The default is 0.

Command Modes CEE map configuration mode

Description Use this command to remap 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. Valid values range from 0 through 6. Default is 0.

Defaults See Operands.

Command Modes CEE map configuration mode

Description Use this command to remap 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 want 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, a warning 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**

rename (Access Gateway mode)

Provides a name for a port group or renames a port group in Access Gateway mode.

Synopsis **rename** *pg_name*

Operands *pg_name* Port group name

Defaults None

Command Modes Port Grouping configuration mode

Description Renames a specific port group identifier.

Usage Guidelines You must be in Port Grouping configuration mode for the specific port group to use this command. The *pg_name* cannot exceed 64 characters,.

Examples Renaming port group pg-1 to pg-array24.

```
sw0(config-rbridge-id-3-ag-pg-1)# rename pg-array24
```

See Also **show ag pg, pg**

resequence access-list

Specifies the renumbering of the rules in a MAC or IP ACL.

Synopsis **resequence** {ip | ipv6 | mac} **access-list** *name* [*seq_num* | *increment*]
no resequence {ip | ipv6 | mac} **access-list** *name* [*seq_num* | *increment*]

Operands **ip | ipv6 | mac** Specifies the Layer 2 or Layer 3 ACL bound to an interface.

name Specifies the name of a standard or an extended ACL. A maximum of 63 characters is allowed.

seq_num Specifies the starting sequence number in the ACL. Valid values range from 1 through 65535.

increment Specifies a value to increment the sequence number between rules. Valid values range 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.

Use the **no** form of this command to remove the ACL binding sequence.

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 802.1Q VLANs that cannot be created by means of the **interface vlan** command.

Synopsis **reserved-vlan** *start-VLAN-ID end-VLAN-ID*

Operands *start-VLAN-ID* Valid values range from 1 through 4090.
end-VLAN-ID Valid values range from 1 through 4090.

Defaults For a Brocade VDX 6720 switch, the default reserved space is 128 VLANs, and is equal to sum of the number of maximum allowed port channels and the number of interfaces on a Brocade VDX 6720-60 switch. Presently, VLANs from 3960 through 4090 are reserved.
For a Brocade VDX 8770 switch, the default reserved VLAN space is 4. VLANs 4087 through 4090 are reserved on this switch.

Command Modes Global configuration mode

Description Use this command to specify the range of 802.1Q VLANs that cannot be created by means of the **interface vlan** command.

NOTE

This command does not apply to service or transport VFs in a Virtual Fabrics context (VLAN ID > 4095).

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, interface vlan**

restrict-flooding

Restricts the flooding of egress BUM traffic from a port-profile port.

Synopsis **restrict-flooding**
 no restrict-flooding

Operands None

Defaults None

Command Modes Port profile configuration mode

Description Use this command to restrict the egress BUM traffic from a port-profile port. The default behavior would be to allow the egress BUM traffic.

This command is applicable only on the default profile and automatically applied to all the port-profile-ports on the switch.

This command only blocks the egress BUM traffic. Ingress traffic, known as unicast traffic, is not impacted.

Usage Guidelines Use the **no restrict-flooding** version of this command to remove the restriction.

Examples None

See Also None

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. Valid values range from 0 through 255.

Defaults The default is 0.

Command Modes Protocol Spanning Tree MSTP configuration mode

Description Use this command to specify the configuration revision number.

Usage Guidelines If MSTP is enabled over VCS, this command must be executed on all R Bridges.
Enter **no revision** to return to the default setting.

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 (OSPF)

Configures compatibility with RFC 1583.

Synopsis **rfc1583-compatibility**
 no rfc1583-compatibility

Operands None

Defaults OSPF is compatible with RFC 1583 (OSPFv2).

Command Modes OSPF VRF router configuration mode

Description Use this command to enable or disable compatibility with RFC 1583. OSPF is compatible with RFC 1583 (OSPFv2) and 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 Enter **no rfc1583-compatibility** to disable compatibility with RFC 1583.

Examples To disable compatibility with RFC 1583:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# rfc1583-compatibility
```

See Also None

rfc1587-compatibility (OSPF)

Configures compatibility with RFC 1587.

Synopsis **rfc1587-compatibility**
 no rfc1587-compatibility

Operands None

Defaults OSPF is compatible with RFC 1587 (OSPFv2).

Command Modes OSPF VRF router configuration mode

Description Use this command to enable or disable compliance with RFC 1587, the original NSSA specification. Only part of the newer RFC 3101 is supported—the “no-summary” parameter and the handling of default-route LSAs when “no summary” is enabled.

Usage Guidelines Enter **no rfc1587-compatibility** to disable compatibility with RFC 1587.

Examples To disable compatibility with RFC 1587:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# no rfc1587-compatibility
```

See Also None

rib-route-limit (BGP)

Limits the maximum number of BGP Routing Information Base (RIB) routes that can be installed in the Routing Table Manager (RTM).

Synopsis **rib-route-limit** *num*
 no rib-route-limit *num*

Operands *num* Decimal value for maximum number of RIB routes to be installed in the RTM. Range is from 1 through 65535.

Defaults This option is disabled. There is no limit.

Command Modes BGP Address-Family IPv4 Unicast configuration mode

Description Use this command to limit the maximum number of BGP RIB routes that can be installed in the RTM.

Usage Guidelines Use the **no** form of this command to restore the default.

Examples To configure the device limit the maximum number of BGP RIB routes that can be installed in the RTM:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# rib-route-limit 10000
```

See Also None

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]]*
no rmon alarm

Operands

<i>index</i>	Specifies the RMON alarm index. Valid values range from 1 through 65535.
<i>snmp_oid</i>	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.
<i>interval seconds</i>	Specifies the RMON alarm sample interval in seconds. Valid values range 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. Valid values range from 0 through 4294967295.
event number	Specifies the event for the rising alarm. Valid values range from 1 through 65535.
falling-threshold value	Specifies the RMON alarm falling threshold. Valid values range from 0 through 4294967295.
event number	Specifies the event for the rising alarm. Valid values range from 1 through 65535.
owner name	Specifies the identity of the owner. The maximum number of characters is 32.

Defaults No alarms are configured.

Command Modes Global configuration mode

Description Use this command to set alarm conditions.

Usage Guidelines Enter **no rmon alarm** to disable the alarm conditions.

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 rmon collection history *number*

Operands *number* Specifies the RMON collection control index value. Valid values range from 1 through 65535.

buckets *bucket_number* Specifies the maximum number of buckets for the RMON collection history. Valid values range from 1 through 65535.

interval *seconds* Specifies the alarm sample interval in seconds. Valid values range 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 RMON history collection is not enabled.

Command Modes Interface subtype configuration mode

Description Use this command to collect periodic statistical samples of Ethernet group statistics on a specific interface for later retrieval.

Usage Guidelines Enter **no rmon collection history** *number* 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 10-gigabit Ethernet 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. Valid values range from 1 through 65535.
 owner name Specifies the identity of the owner.

Defaults RMON statistic collection is not enabled.

Command Modes Interface subtype configuration mode

Description Use this command to collect Ethernet group statistics on a specific interface.

Usage Guidelines Enter **no rmon collection stats** *number* 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 10-gigabit Ethernet 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

<i>index</i>	Specifies the RMON event number. Valid values range from 1 through 65535.
<i>description word</i>	Specifies a description of the event.
log	Generates an RMON log when an event is triggered.
<i>owner name</i>	Specifies the owner of the event. The <i>name</i> string must be between 1 and 32 characters in length.
trap word	Specifies the SNMP community or string name to identify this trap.

Defaults No events are 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.

Usage Guidelines Enter **no rmon event** to remove the event configuration.

Examples To configure an RMON event:

```
switch(config)# rmon event 2 log description "My Errorstoday" owner gjack
```

See Also `show rmon history`

role name

Creates or modifies a user role.

Synopsis **role name** *role_name* [**desc** *description*]
no role name

Operands *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 mark ('), double quotation mark ("), 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.

Enter **no role name** to set 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
```

See Also **rule, show running-config role, show running-config rule**

route-map

Creates or deletes a route map instance, with a variety of options.

Synopsis **route-map** *name* [**permit** | **deny**] *instance_number* | [**continue** *sequence number*]
no route-map *name* [**permit** | **deny**] *instance_number* | [**continue** *sequence number*]

Operands *name* The name of the route map. The string must be between 1 and 63 ASCII characters in length.

permit Allows a matching pattern

deny Disallows a matching pattern.

instance_number The instance ID. The range is from 1 through 65535.

continue Use a “continue” clause to allow for more programmable policy configuration and route filtering, with capability to execute additional entries in a route map after an entry is executed with successful “match” and “set” clauses.

sequence_number The sequence ID. The range is from 1 through 65535.

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command to create or delete a route map instance.

 This command is used in conjunction with other commands.

 For details on **match** commands, refer to the following commands:

- **match (route map)**
- **match access-list**
- **match as-path**
- **match community**
- **match interface**
- **match ip address**
- **match ip next-hop**
- **match metric**
- **match protocol bgp**
- **match route-type**
- **match tag**

For details on **set** commands, refer to the following commands:

- **set as-path**
- **set as-path prepend**
- **set automatic-tag**
- **set comm-list**

- **set community**
- **set cos traffic-class**
- **set dscp**
- **set dampening**
- **set distance**
- **set ip next-hop**
- **set local-preference**
- **set metric**
- **set metric-type**
- **set origin**
- **set route-type**
- **set tag**
- **set weight**

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. Enter no route-map <i>name</i> to remove the route-map name.
Examples	None
See Also	All commands listed under Description, above.

router bgp

Enables BGP4 routing.

Synopsis **router bgp**

no router bgp

Operands None

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command to enable BGP4 routing.

Usage Guidelines Use the **no** form of this command to disable BGP4 routing.

Examples To enable BGP4 routing:

```
switch(config)# rbridge-id 10  
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)#
```

See Also None

router ospf

Enables and configures the Open Shortest Path First (OSPF) routing protocol over virtual forward and routing (VRF).

Synopsis **router ospf** [*vrf name*]
no router ospf

Operands **vrf name** The name of the non-default VRF to connect.

Defaults Enabled

Command Modes Global configuration mode

Description Use this command to enable the OSPF routing protocol and enter OSPF VRF router configuration mode. With NetworkOS4.0 and later, OSPF can run over multiple Virtual Forwarding and Routing (VRF) mechanisms. OSPF maintains multiple instances of the routing protocol to exchange route information among various VRF instances.

Usage Guidelines Enter **no router ospf** to delete all current OSPF configuration and to block any further OSPF configuration.

Examples To enable OSPF on a default VRF and to enter OSPF VRF router configuration mode, run the **router ospf** command in RBridge ID configuration mode, as shown in the following example:

```
switch# configure  
switch(config)# rbridge-id 5  
switch(config-rbridge-id-5)#router ospf  
switch(config-router-ospf-vrf-default-vrf)
```

To enable OSPF on a non-default VRF and to enter OSPF VRF router configuration mode, run the **router ospf vrf name** command in RBridge ID configuration mode, as shown in the following example:

```
switch# configure  
switch(config)# rbridge-id 5  
switch(config-rbridge-id-5)#router ospf vrf vrfname  
switch(config-router-ospf-vrf-vrfname)
```

See Also None

router pim

Enables or disables the Protocol Independent Multicast (PIM) routing protocol.

Synopsis **router pim**
 no router pim

Operands None

Defaults The PIM protocol is disabled.

Command Modes RBridge ID configuration mode

Description Use this command to enable or disable the PIM protocol. It launches the PIM router configuration mode.

Usage Guidelines Enter **exit** to exit this mode.

Examples To enable the PIM protocol:

 switch(config-rbridge-id-128)# **router pim**

See Also None

route-target

Imports or exports the routes for the router-id.

Synopsis **route-target** [*admin-value:arbitrary-value*] [**export** | **import**]

Operands	<i>admin-value</i>	The administrative number assigned to the route. This can be a local ASN number or an IP address. The ASN number can be either a 2 byte (from 0 through 65535) or a 4 byte number from 0 through 4294967295).
	<i>arbitrary-value</i>	An arbitrary number you choose. The range of valid values is from 0 through 65535 if the ASN is 2 byte, or from 0 through 4294967295 if the ASN is 4 byte.
	export	Exports the routes.
	import	Import the routes.

Defaults None

Command Modes VRF configuration mode

Description Use this command to import or export the routes for the router-id for the specified VRF.

Usage Guidelines None

Examples None

See Also **vrf, ip router-id**

rp-address

Adds or removes a static rendezvous point.

Synopsis **rp-address** *A.B.C.D*
 no rp-address

Operands *A.B.C.D* The IP address that should be designated as the rendezvous point router.

Defaults No interface is configured as the rendezvous point candidate.

Command Modes PIM router configuration mode

Description Use this command to add or remove a static rendezvous point address for a PIM domain. Since prefix-lists are not supported, the address is assumed to be the rendezvous point for 224.0.0.0/4 address range.

Usage Guidelines Enter **no rp-address** to disable this feature.

Examples Setting the IP address to 12.12.12.12.

 switch(conf-pim-router)# **rp-address 12.12.12.12**

See Also router pim

rspan-vlan

Configures the VLAN to support RSPAN (Remote Switched Port Analyzer) traffic analysis.

Synopsis **rspan-vlan**

Operands None

Defaults None

Command Modes VLAN configuration mode

Description This command configures the VLAN to support RSPAN. RSPAN extends SPAN by enabling remote monitoring of multiple switches across your network.

Usage Guidelines All participating switches must be trunk-connected at Layer 2, and RSPAN must be configured on all the switches participating in the RSPAN session.

Examples Typical execution of this command.

```
switch(config)# interface vlan 300  
switch(config-vlan-300)# rspan-vlan
```

See Also **interface vlan**, **show vlan**

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. Valid values range from 1 through 512.

action **accept** | **reject** Specifies whether the user is accepted or rejected while attempting to execute the specified command. The default value is **accept**.

operation **read-only** | **read-write** Specifies the type of operation permitted. The default value is **read-write**.

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 with a space. RBAC support is provided only for the following commands with parameters: copy, clear, interface, and protocol.

Defaults The default for **action** is **accept**. The default for **operation** is **read-write**.

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.

Enter **no rule** *index* to remove the specified rule.

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 name**, **show running-config role**, **show running-config rule**

scheduler

Specifies the scheduling attributes along with the TC shape rate.

Synopsis `scheduler sp_count [shape_rate | [shape_rate ... shape_rate] dwrr [weight | weight ... weight]`

Operands

<code>sp_count</code>	Specifies how many strict priority queues for each port scheduler. The range of valid values is from 0 through 8.
<code>shape_rate</code>	Specifies the shape rate on strict priority queues. The range of valid values are from 28000 kbps to the maximum interface speed.
<code>dwrr weight</code>	Specifies the dwrr weight percentage for the queue. The range of valid values is from 1% through 100%, and the sum of all dwrr weights should not exceed 100%.

Defaults None

Command Modes Policy-map configuration mode

Description Use this command to specify the scheduling attributes along with the TC shape rate.

There are total eight queues are present on an interface. The number of dwrr queues present depends on the SP_COUNT value. For example if the SP_COUNT is two, then there are two strict priority queues and six dwrr queues.

Usage Guidelines This command is allowed only for the Egress direction.

This command can only be configured in for the **class class-default** command.

This command is mutually exclusive of the **port-shape** and **police** commands.

Examples Typical command example:

```
switch(config)#policy-map mutation
switch(config-policymap)#class class-default
switch(config-policyclass)# scheduler 3 31000 32000 33000 dwrr 20 20 20 10 10
```

See Also `class`, `policy-map`

secpolicy activate

Activates the defined switch connection control (SCC) policy and its member set.

Synopsis **secpolicy activate** [**rbridge-id** *rbridge-id* | **all**]

Operands **rbridge-id** Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id Specifies a unique identifier for a node.

all Specifies all identifiers for a node.

Defaults 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 Use this command to activate 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** parameter 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 Brocade VDX 6730 switches.

Examples Standalone mode

To activate the defined SCC policy:

```
switch# secpolicy activate
```

VCS mode

```
switch# secpolicy activate rbridge-id 3
```

See Also **secpolicy defined-policy**

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 Any switch is allowed to join the fabric.
 The SCC policy does not exist until it is created.

Command Modes Global configuration mode
 RBridge ID 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 This command is not distributed across the cluster. The RBridge ID of the node should be used to configure policy configurations.

Although the **active-policy** is listed under the possible completions of **secpolicy** command, the defined-policy parameter should be used to create or add policy or members.

Entering **secpolicy activate** activates the policy.

You can add multiple WWNs separated by a comma.

After you configure the defined SCC_POLICY, run **secpolicy activate** to apply the changes to the active policy set.

This command is supported only on Brocade VDX 6730 switches.

Enter **no secpolicy defined-policy SCC_POLICY member-entry switch_wwn** to remove a switch (WWN) from the defined policy member set.

Enter **no secpolicy defined-policy SCC_POLICY** to remove the SCC policy, along with all of the defined policy members.

Examples Standalone mode

To create the defined SCC policy:

```
switch(config)# secpolicy defined-policy SCC_POLICY
switch(config-defined-policy-SCC_POLICY)# exit
```

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
switch(config-member-entry-10:00:00:05:1e:00:69:01)# exit
```

2 secpolicy defined-policy

```
switch(config-defined-policy-SCC_POLICY)# exit
```

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
```

VCS mode

To create the defined SCC policy:

```
switch(config)# rbridge-id 3  
switch(config-rbridge-id-3)# secpolicy defined-policy SCC_POLICY  
switch(config-defined-policy-SCC_POLICY)# exit
```

To add a switch WWN to the policy set:

```
switch(config)# rbridge-id 3  
switch(config-rbridge-id-3)# secpolicy defined-policy SCC_POLICY member-entry  
10:00:00:05:1e:00:69:00  
switch(config-member-entry-10:00:00:05:1e:00:69:00)# exit  
switch(config-defined-policy-SCC_POLICY)# exit  
switch(config-rbridge-id-3)# exit
```

To remove an entry from the policy list of rbridge id 3:

```
switch(config)# rbridge-id 3  
switch(config-rbridge-id-3)# no secpolicy defined-policy SCC_POLICY member-entry  
10:00:00:05:1e:00:69:01
```

To remove the SCC_POLICY entry of rbridge id 3:

```
switch(config)# rbridge-id 3  
switch(config-rbridge-id-3)# no secpolicy defined-policy SCC_POLICY
```

See Also **secpolicy activate**

security-profile (AMPP)

Activates the security-profile mode for AMPP.

Synopsis **security-profile**
 no security-profile

Operands None

Defaults None

Command Modes Port-profile configuration mode

Description Use this command to activate the security-profile mode for AMPP. This mode allows configuration of security attributes of a port-profile.

Usage Guidelines Enter **no security-profile** to remove the profile.

Examples To activate the security-profile mode for AMPP:

```
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** *seq-value* {**permit** | **deny** | **hard-drop**} *ip-protocol* {**any** | *SIP mask* | **host** *SIP*} [{**eq** | **gt** | **lt** | **neq** | **range**} *sport number*] {**any** | *DIP mask* | **host** *DIP*} [{**eq** | **gt** | **lt** | **neq** | **range**} *dport number*] [*dscp value*] [**ack** **fin** **rst** **sync** **urg** **psh**] [**count**] [**log**]

no seq *seq-value* {**permit** | **deny** | **hard-drop**} *ip-protocol* {**any** | *SIP mask* | **host** *SIP*} [{**eq** | **gt** | **lt** | **neq** | **range**} *sport number*] {**any** | *DIP mask* | **host** *DIP*} [{**eq** | **gt** | **lt** | **neq** | **range**} *dport number*] [*dscp value*] [**ack** **fin** **rst** **sync** **urg** **psh**] [**count**] [**log**]

Operands	<i>seq-value</i>	Specifies the sequence number for the rule. Valid values range from 0 through 65535.
	permit	Specifies rules to permit traffic.
	deny	Specifies rules to deny traffic.
	hard-drop	Overrides the trap behavior for control frames and data frames such as echo request (ping). See the Usage Guidelines.
	<i>ip-protocol</i>	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 <i>Source_IP_ADDRESS</i>	Specifies the source host IP address for which to set permit or deny conditions.
	<i>Source_IP_mask</i>	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 two 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.
	<i>source_port_number</i>	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 numbers 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 you can mask for any bit. For example, 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. Valid values range 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 parameter is only available with permit and deny.
- remark comment** An ASCII string 0 to 256 characters in length.

Defaults No IP ACLs are configured.

Command Modes Feature Access Control List configuration mode

2 seq (extended IP ACLs)

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.

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.

Enter **no seq** *value* to remove a rule from the IP ACL.

If an ACL is set up to deny a specific host or range (such as “seq 2 deny host 10.9.106.120”), the VDX still responds to ping unless the **hard-drop** operand is added (such as “seq 20 hard-drop icmp any any”).



CAUTION

The use of ‘hard-drop’ can prevent the trapping of control frames. As a result, it could interfere with normal operations of the protocols.

If no sequence value is specified, the rule is added to the end of the list.

IP ACL logging of hits is not supported on the VDX 6720 switch.

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** | A:B:C:D:E:F:H:I/prefix_len | **host** *SIP_address* | *SIP_address mask*] [**count**] [**log**]

no seq *value* {**deny** | **permit** | **hard-drop**} [**any** | A:B:C:D:E:F:H:I/prefix_len | **host** *SIP_address* | *SIP_address mask*] [**count**] [**log**]

Operands	value	Specifies the sequence number for the rule. Valid values range from 0 through 4294967295.
	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 <i>SIP_address</i>	Specifies the source host IP address for which to set permit or deny conditions.
	<i>SIP_mask</i>	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 parameter is only available with permit and deny.
	remark <i>comment</i>	An ASCII string 0 to 256 characters in length.

Defaults 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.

Usage Guidelines Enter **no seq** *value* {**deny** | **permit** | **hard-drop**} [**any** | A:B:C:D:E:F:H:I/prefix_len | **host** *SIP_address* | *SIP_address mask*] [**count**] [**log**] to remove a rule from the IP ACL.

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. Valid values range 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. Valid values range 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 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.

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.

Enter **no seq** *value* to remove a rule from the MAC ACL.

Hard-drop can prevent trapping of control frames. As a result, it could interfere with normal operations of the protocols.

If no sequence value is specified, the rule is added to the end of the list.

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(config-macl-ext)# seq 100 deny 0022.3333.4444 0022.3333.5555 ipv4 count  
switch(config-macl-ext)# seq 1000 permit 0022.3333.4444 0022.3333.5555 ipv4 count
```

To delete a rule from a MAC extended ACL:

```
switch(config-macl-ext)# no seq 100
```

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

seq (standard MAC ACLs)

Inserts a rule anywhere in the MAC ACL.

Synopsis **seq** *value* [**deny** | **permit** | **hard-drop**] [**any** | **host** *MAC_ADDRESS* | *MAC_ADDRESS*] [**count**]
no seq *value*

Operands

<i>value</i>	Specifies the sequence number for the rule. Valid values range from 0 through 65535.
permit	Specifies rules to permit traffic.
deny	Specifies rules to deny traffic.
any	Specifies any source MAC address.
host <i>MAC_ADDRESS</i>	Specifies the source host MAC address for which to set permit or deny conditions. Use the format HHHH.HHHH.HHHH.
<i>MAC_ADDRESS</i>	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.
hard-drop	Overrides the trap behavior for control frames and data frames such as echo request (ping).

Defaults 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.

Usage Guidelines Enter **no seq** *value* to remove a rule from the MAC ACL.

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 access-list

service password-encryption

Enables or disables password encryption.

Synopsis **service password-encryption**
 no service password-encryption

Operands None

Defaults Default value is service password-encryption.

Command Modes Global configuration mode

Description Use this command to enable encryption for all user account passwords.

Usage Guidelines Enter **no service password-encryption** to disable password encryption.

Examples To enable password encryption:
 switch(config)# **service password-encryption**

 To disable password encryption:
 switch(config)# **no service password-encryption**

See Also **show running-config password-attributes**

service-policy

Binds a policy-map to an interface.

Synopsis	service-policy in out <i>policy-map name</i> no service-policy in out	
Operands	in	Binds policy-map to inbound traffic.
	out	Binds policy-map to outbound traffic.
	<i>policy-map name</i>	Name of the policy-map.
Defaults	No service policy is created.	
Command Modes	Interface subtype configuration mode	
Description	Use this command to apply a policy-map containing a class-map with specific Policer parameters and match critters to a switch interface. The policy-map must be configured before you can apply it (refer to the description of the policy-map command).	
Usage Guidelines	Enter no service-policy in out while in the applicable interface subconfiguration mode to remove the service policy.	
	NOTE This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.	
Examples	To create a service-policy for outbound traffic on a specific 10-gigabit Ethernet 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 10-gigabit Ethernet 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 10-gigabit Ethernet 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 as-path

Sets a prepended string or a tag for a BGP AS-path attribute in a route-map instance.

Synopsis **set as-path** [**prepend** *string* | **tag**]
 no set as-path [**prepend** *string* | **tag**]

Operands **prepend** Prepends the string to the AS-path.
 string AS numbers. Range is from 1 through 4294967295.
 tag Sets a route tag.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set a prepended string or a tag for a BGP AS-path attribute in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

set as-path prepend

Prepends an AS4 number to an AS path, makes the AS number a tag attribute for a route map, and provides a variety of route-management options.

Synopsis	set as-path prepend <i>as-num, as-num, . . . as-num</i> [automatic-tag] [comm-list <i>acl</i> delete] [community <i>num:num</i> <i>num</i> additive internet local-as no-advertise no-export] [dampening [<i>half-life</i> <i>reuse</i> <i>suppress</i> <i>max-suppress-time</i>]] [ip next hop <i>ip-addr</i>] [ip next-hop peer-address] [local-preference <i>num</i>] [metric [add assign none sub]] [metric-type [<i>type-1</i> <i>type-2</i>]] external [metric-type internal] [origin igp incomplete] [tag] [weight <i>num</i>] no set as-path prepend <i>as-num, as-num, . . . as-num</i>	
Operands	automatic-tag	Calculates and sets an automatic tag for the route.
	comm-list <i>acl</i> delete	Deletes a community from the community attributes field for a BGP4 route.
	community	Sets the community attribute for the route to the number or well-known type specified. Possible values are <i>num:num</i> , Internet, no-export, local-as, no-advertise.
	<i>num:num</i>	Specific community member.
	additive	Adds a community to the already existing communities.
	internet	The Internet community.
	local-as	Local sub-AS within the confederation. Routes with this community can be advertised only within the local sub-AS.
	no-advertise	Routes with this community cannot be advertised to any other BGP4 devices at all.
	no-export	Community of sub-ASs within a confederation. Routes with this community can be exported to other sub-ASs in the same confederation but not outside the confederation to other ASs or otherwise sent to EBGp neighbors.
	dampening	Sets dampening parameters for the route.
	<i>half-life</i>	Number of minutes after which the route penalty becomes half its value.
	<i>reuse</i>	Specifies how low a route penalty must become before the route becomes eligible for use again after being suppressed.
	<i>suppress</i>	Specifies how high a route penalty can become before the device suppresses the route.
	<i>max-suppress-time</i>	Specifies the maximum number of minutes that a route can be suppressed regardless of how unstable it is.
	ip next hop	Sets the next-hop IP address for a route that matches the match statement in the route map.
	<i>ip-addr</i>	IPv4 address in dotted-decimal notation.

ip next-hop peer-address

Sets the BGP4 next hop for a route to the neighbor address.

local-preference

Sets the local preference for the route.

num

Range is from 0 through 4294967295.

metric

Sets the MED (metric) value for the route. Range is from 0 through 4294967295. The default MED value is 0.

add

Adds to the current metric value.

assign

Replaces the current metric value with a new value.

none

Removes the MED attribute (metric) from the BGP4 route.

sub

Subtracts from the current metric value.

metric-type

Changes the metric type of the route redistributed into OSPF.

type-1

Type 1 route.

type-2

Type 2 route.

external

External Type 1 or Type 2 route.

metric-type internal

Sets route MED attribute to same value as the IGP metric of the BGP4 next-hop route, for advertising a BGP4 route to an EBGp neighbor.

next-hop

Sets IPv4 address of the next hop.

ip-addr

IPv4 address in dotted-decimal notation.

origin

Sets the route's origin.

igp

Sets origin to IGP.

incomplete

Sets origin to INCOMPLETE.

tag

Keyword that makes the ASN an AS-path tag attribute. (Applies only to routes redistributed into OSPF.)

weight

Sets the weight for the route.

num

Range is from 0 through 4294967295.

Defaults

None

Command Modes

Route-map configuration mode

Description

Use this command to prepend an AS4 number to an AS path, make the AS number a tag attribute for a route map, and set a variety of other route-management options.

Usage GuidelinesUse the **no** form of this command to remove the configuration.**Examples**

To prepend an AS4 number:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# route-map myroutes
switch(config-route-map myroutes)# set as-path prepend 7701000
```

See Also**route-map**

set automatic-tag

Sets the route-map tag value.

Synopsis **set automatic-tag** *value*

Operands *value* The value for the computed tag.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set an automatically computed tag value in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

set comm-list

Sets a BGP community list for deletion in a route-map instance.

Synopsis **set comm-list** *name*
 no set comm-list *name*

Operands *name* BGP community list name. Range is from 1 through 32 ASCII characters.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set a BGP community list for deletion in a route-map instance.

Usage Guidelines Use the **no** version of this command to disable this feature.

Examples None

See Also **route-map**

set community

Sets a BGP community attribute in a route-map instance.

Synopsis **set community** [*community-number* | **local-as** | **no-advertise** | **no-export** | **none**]
 no set community *community-number*

Operands *community-number* BGP community number, in two format options:
 (1) Range is from 1 through 4294967295.
 (2) Format is AA:NN, where AA is the AS number, and NN is a locally
 significant number.

local-as Do not send outside local AS (well-known community).

no-advertise Do not advertise to any peer (well-known community).

no-export Do not export to next AS (well-known community).

none Sets no community attribute.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set a BGP community list attribute in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

set cos traffic-class

Specifies the User-Priority field value in VLAN header and traffic-class queuing value when a packet matches a flow.

Synopsis **set cos {0..7} traffic-class {0..7}**
no set cos {0..7} traffic-class {0..7}

Operands **0..7}** Modifies the Class of Service (CoS) value in the VLAN header of classified traffic, or assigns a queue to the classified traffic. The range of valid values is from 0 through 7.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to specify the User-Priority field value in VLAN header and traffic-class value when a packet matches a flow.

Usage Guidelines None

Examples

```
switch(config)# policy-map p1
switch(config-policymap)# class c1
switch(config-policyclass)# set cos 4 traffic-class 3
```

See Also **class, policy-map**

set dscp

Specifies the DSCP field value in IP header when a packet matches a flow.

Synopsis **set dscp {0..63}**
 no set dscp {0..63}

Operands **0..63** The DSCP value in the IP header of the classified traffic. The range of valid values is from 0 through 63.

Defaults None

Command Modes Route-map configuration mode

Description You can specify the DSCP field value in IP header when a packet matches a flow.

Usage Guidelines None

Examples `switch(config)#policy-map p1`
 `switch(config-policymap)#class c1`
 `switch(config-policyclass)#set dscp 56`

See Also **class, policy-map**

set dampening

Sets a BGP route-flap dampening penalty in a route-map instance.

Synopsis **set dampening** *number*
 no set dampening *number*

Operands *number* Half-life in minutes for the penalty. Range is from 1 through 45.

Defaults The default is 15.

Command Modes Route-map configuration mode

Description Use this command to set a BGP route-flap dampening penalty in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

set distance

Sets the administrative distance for matching OSPF routes in route-map instance.

Synopsis **set distance** *value*
 no set distance

Operands *value* Administrative distance for the route. Range is from 1 through 254.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set the route administrative distance in a route-map instance.

Usage Guidelines None

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 interface null0

Drops traffic when the null 0 statement becomes the active setting.

Synopsis **set ip interface null0**
 no set ip interface null0

Operands None

Defaults None

Command Modes Route-map configuration mode

Description Use this command to drop traffic when the null 0 statement becomes the active setting as determined by the route-hop selection process.

Usage Guidelines The **no** command setting deletes the matching filter from the ACL.

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 ip next-hop

Sets the IPv4 address of the next hop in a route-map instance.

Synopsis **set ip** [**global** | **vrf** *vrf-name*] **next-hop** *A.B.C.D*
no set ip next-hop *A.B.C.D*

Operands	<i>A.B.C.D</i>	IPv4 address of the next hop.
	global	Specifies that the next specified hop address is to be resolved from the global routing table.
	vrf <i>vrf-name</i>	Specifies from which VRF routing table the specified next hop address will be resolved.
	next hop <i>A.B.C.D</i>	Sets the next hop to which to route the packet. The next hop must be adjacent.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to specify the IPv4 address of the next hop in a route-map instance.

Usage Guidelines Use the **no** form of this command to delete the matching filter from the ACL.

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 local-preference

Sets a BGP local-preference path attribute in a route-map instance.

Synopsis **set local-preference** *number*
 no set local-preference

Operands *number* Range is from 0 through 4294967295.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set a BGP local-preference path attribute in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

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 current route metric.
	assign	Replaces the current route metric with this value.
	sub	Subtracts the value from the current route metric.
	none	Removes the current route metric.
	<i>value</i>	Range is from 0 through 4294967295.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to modify or remove the current route metric in a route-map instance.

Usage Guidelines None

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 metric-type

Sets a variety of metric types for destination routing in a route-map instance.

Synopsis **set metric-type** [external | internal | type-1 | type-2]
 no set metric-type [external | internal | type-1 | type-2]

Operands	external	IS-IS external metric
	internal	IGP internal metric to BGP MED
	type-1	OSPF external type-1 metric
	type-2	OSPF external type-2 metric

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set a variety of metrics for destination routing in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

set origin

Sets a BGP origin code in a route-map instance.

Synopsis **set origin** [igp | incomplete]
no set origin [igp | incomplete]

Operands **igp** Local IGP
 incomplete Unknown heritage

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set a BGP origin code in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

set-priority

Optional command for configuring the priority map of a class-map.

Synopsis **set-priority** *priority-map-name*
 no set-priority *priority-map-name*

Operands *priority-map-name*The priority-map name that you are including in the policy-map. Refer to the description of the **police-priority-map** command.

Defaults None

Command Modes Class-map configuration mode

Description This command configures the priority map of a class-map.

Usage Guidelines Only the **police cir** and **cbs** commands are mandatory for configuring a class-map.

If the optional parameters for a class-map are not set, they are treated as disabled. To delete parameters for a class-map, you must delete all policer parameters while in the policy-map class configuration mode using the **no police cir** command.

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

Use the **no** version of this command to remove the parameter from the class-map.

Examples

```
switch(config-policymap)# class default
switch (config-policymap-class)# police cir 40000
switch (config-policymap-class)# set-priority default
```

See Also **cbs, conform-set-dscp, conform-set-prec, conform-set-tc, ebs, eir, exceed-set-dscp, exceed-set-prec, exceed-set-tc, police cir, police-priority-map, policy-map, qos cos, service-policy**

set route-type

Sets a route type in a route-map instance.

Synopsis **set route-type** [**internal** | **type-1** | **type-2**]
 no set route-type

Operands	internal	Internal route type
	type-1	OSPF external route type 1
	type-2	OSPF external route type 2

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set a route type in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

set tag

Sets the route tag value in a route-map instance.

Synopsis **set tag** *value*
 no set tag *value*

Operands *value* The tag clause value for the route-map. Range is from 0 through 4294967295.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to set the route tag value in a route-map instance.

Usage Guidelines Enter **no set tag** *value* 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**

set weight

Sets a BGP weight for the routing table in a route-map instance.

Synopsis **set weight** *number*
 no set weight *number*

Operands *number* Weight value. Range is from 0 through 65535.

Defaults None

Command Modes Route-map configuration mode

Description Use this command to set a BGP weight for the routing table in a route-map instance.

Usage Guidelines None

Examples None

See Also **route-map**

sflow collector

Identifies the sFlow collectors to which sFlow datagrams are forwarded.

Synopsis **sflow collector** [*IPv4 address* | *IPv6 address*]

no sflow collector [*IPv4 address* | *IPv6 address*]

Operands *IPv4 address* Specifies an IPv4 address in dotted-decimal format for the collector.
IPv6 address Specifies an IPv6 address 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.

Usage Guidelines You can only specify up to five sFlow collectors.

Enter **no sflow collector** [*IPv4 address* | *IPv6 address*] to reset the specified collector address to a null value.

Examples To identify the sFlow collectors for an IPv4 address to which sFlow datagrams are forwarded:

```
switch(config)# sflow collector 192.10.138.176
```

To identify the sFlow collectors for an IPv6 address and port to which sFlow datagrams are forwarded:

```
switch(config)# sflow collector 3ff3:1900:4545:3:200:f8ff:fe21:67cf : 6343
```

See Also None

sflow enable (global version)

Enables sFlow globally.

Synopsis **sflow enable**
 no sflow enable

Operands None

Defaults sFlow is disabled on the system.

Command Modes Global configuration mode

Description Use this command to enable sFlow globally.

Usage Guidelines This command is supported on physical ports only.

On a Brocade VDX 8770, SPAN and sFlow can be enabled at the same time.

On a Brocade VDX 6720, SPAN and sFlow *cannot* be enabled at the same time.

Enter **no sflow enable** to disable sFlow globally.

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 sFlow is disabled on all interfaces.

Command Modes Interface subtype configuration mode

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 a Brocade VDX 8770 switch, SPAN and sFlow can be enabled at the same time.

On the Brocade VDX 6720 switch, SPAN and sFlow *cannot* be enabled at the same time.

Enter **no sflow enable** to disable sFlow on an interface.

Examples To enable sFlow on a specific 40-gigabit Ethernet 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. Valid values range from 1 through 65535 seconds.

Defaults The default is 20.

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.

Usage Guidelines Enter **no sflow polling interval** *interval_value* to return to the default value.

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. Valid values range from 1 through 65535.

Defaults The default is 20.

Command Modes Interface subtype configuration mode

Description Use this command to configure the polling interval for an interface. The interval is the maximum number of seconds between successive samples of counters to be sent to the collector.

Usage Guidelines Enter **no sflow polling interval** to return to the default value.

Examples To set the polling interval to 135 seconds on a specific 40-gigabit Ethernet 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. Valid values range from 2 through 16777215 packets.

Defaults The default is 32768.

Command Modes Global configuration mode

Description Use this command to change the current global default sampling rate. Sample-rate is the average number of packets skipped before the sample is taken.

Usage Guidelines Enter **no sflow sample-rate** 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. Valid values range from 2 through 16777215 packets.

Defaults The default is 32768.

Command Modes Interface subtype configuration mode

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. The default sampling rate of an interface is set to the same value as the current global default sampling rate.

Usage Guidelines This command changes the sampling rate for an interface.
Enter **no sflow sample-rate** to return to the default setting.

Examples To change the sampling rate to 4096 packets on a specific 40-gigabit Ethernet 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)

sflow-profile

Establishes an sFlow profile name and sets a sampling rate.

Synopsis **sflow-profile** {*sflow_profile_name*} {**sample-rate** *sampling_rate*}
no sflow-profile {*sflow_profile_name*}

Operands *sflow_profile_name* Name of an sFlow profile for sampling rates. The maximum number of characters is 64.

sample-rate Selects a sampling rate.

sampling_rate Specifies a sampling rate. Range is from 2 through 8388608 packets, in powers of 2 only. The default is 32768 packets.

Defaults This command is disabled.

Command Modes Global configuration mode

Description Use this command to establish an sFlow profile and set a sampling rate.

Usage Guidelines Use the **no** form of this command to disable an sFlow profile.

Examples To establish an sFlow profile and set a sampling rate of 4096:

```
switch(config)# sflow mysflowprofile sample-rate 4096
```

See Also None

sfp breakout

Displays the QSFP port breakout configurations.

Synopsis **sfp breakout**
 no sfp breakout

Operands None

Defaults Breakout mode is set to disabled.

Command Modes Connector configuration mode

Description Use this command to display the QSFP port breakout configuration for the specified QSFP ports.

Usage Guidelines This command is an executable command and it could be executed under connector mode.
This command is destructible and irreversible. After this command, you must execute the “copy running-config startup-config” command, and immediately perform a power-cycle on the corresponding linecard/switch.

NOTE

For the 27x40 GbE line card on a Brocade VDX 8770, a port group must be in performance mode before you can configure one of its ports to breakout mode.

Use the **no sfp breakout** to disable breakout mode and create a single Fo interface.

Examples To enable SFP breakout on a connector:

```
switch(config)# hardware  
switch(config-hardware)#connector 2/0/1  
switch(config-connector-2/0/1)# sfp breakout
```

To disable SFP breakout on a connector:

```
switch(config-connector-2/0/1)# no sfp breakout
```

See Also **show running-config hardware connector, connectorpower-off linecard, power-on linecard**

short-path-forwarding

Enables short-path forwarding on a VRRP router.

Synopsis **short-path-forwarding** [**revert-priority** *number*]
no short-path-forwarding

Operands **revert-priority** *number*

Allows additional control over short-path-forwarding on a backup router. If you configure this option, the revert-priority number acts as a threshold for the current priority of the session, and only if the current priority is higher than the revert-priority will the backup router be able to route frames. The range of revert-priority is 1 to 254.

Defaults Disabled

Command Modes Virtual-router-group configuration mode

Description Use this command to enable short-path forwarding on a VRRP 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 not for VRRP. You can perform this configuration on a virtual Ethernet (VE) interface only.

Enter **no short-path-forwarding** 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** | **ipv6** | **mac**} *name* {**port-channel** *index* | **gigabitethernet** *slot/port* | **tengigabitethernet** *slot/port* | **fortygigabitethernet** *slot/port* | **vlan** *vlan_id* | **ve** *vlan_id*} {**in** | **out**} [**rbridge-id** *rbridge-id* | **all**]

Operands

ip ipv6 mac	Displays the configured rules of either a Layer 2 or Layer 3 ACL.
<i>name</i>	The “name” of the ACL assigned at creation.
port-channel <i>index</i>	Specifies the port-channel index to which the ACL is bound.
gigabitethernet <i>slot/port</i>	Specifies the 1-gigabit Ethernet interface to which the ACL is bound.
tengigabitethernet <i>slot/port</i>	Specifies the 10-gigabit Ethernet interface to which the ACL is bound.
fortygigabitethernet <i>slot/port</i>	Specifies the 40-gigabit Ethernet interface to which the ACL is bound.
vlan <i>vlan_id</i>	Specifies the VLAN interface to which the ACL is bound. Refer to Usage Guidelines below.
ve <i>vlan_id</i>	Specifies the virtual Ethernet (VE) interface to which the ACL is bound. Refer to Usage Guidelines below.
rbridge-id	Specifies one or all RBridge IDs.
<i>rbridge-id</i>	An RBridge ID.
all	Specifies all RBridge IDs.
	Specifies the RBridge ID for node-specific ACL interface details.
in out	Specifies the ACL binding direction (ingress or egress).

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the status of all ACLs bound to a particular 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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 <i>index</i> gigabitethernet <i>slot/port</i> tengigabitethernet <i>slot/port</i> fortygigabitethernet <i>slot/port</i> vlan <i>vlan_id</i> ve <i>vlan_id</i> } { in out } show access-list { ip ipv6 } interface { port-channel <i>index</i> gigabitethernet <i>slot/port</i> tengigabitethernet <i>slot/port</i> fortygigabitethernet <i>slot/port</i> vlan <i>vlan_id</i> ve <i>vlan_id</i> management <i>rbridge-id/port</i> }} { in out }	
Operands	port-channel <i>index</i> Specifies the port-channel index to which the ACL is bound. gigabitethernet <i>slot/port</i> Specifies the 1-gigabit Ethernet interface to which the ACL is bound. tengigabitethernet <i>slot/port</i> Specifies the 10-gigabit Ethernet interface to which the ACL is bound. fortygigabitethernet <i>slot/port</i> Specifies the 40-gigabit Ethernet interface to which the ACL is bound. vlan <i>vlan_id</i> Specifies the VLAN interface to which the ACL is bound. Refer to the Usage Guidelines. ve <i>vlan_id</i> Specifies the virtual Ethernet interface to which the ACL is bound. Refer to the Usage Guidelines. ip Specifies an IPv4 ACL. ipv6 Specifies an IPv6 ACL. <i>rbridge-id</i> Specifies the RBridge ID for node-specific ACL interface details. management <i>rbridge-id/port</i> in out Specifies the ACL binding direction (ingress or egress).	
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to display the status of all ACLs bound to a particular 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.	
Examples	None	
See Also	None	

show access-list ip

Displays summary information for an ACL list.

Synopsis **show access-list** **[[ip** *IP_ACL* **| ipv6** *IP_ACL* **] {in | out}]**

Operands **ip** *IP_ACL* Specifies the IPv4 IP address.

ipv6 *IP_ACL* Specifies the IPv6 IP address.

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

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the status of all ACLs bound to a particular IP address.

Usage Guidelines None

Examples None

See Also **show access-list interface**

show access-list mac

Displays summary information for an ACL list.

Synopsis **show access-list mac {in | out}**

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

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the status of all ACLs bound to a particular IP address.

Usage Guidelines None

Examples None

See Also **show access-list interface**

show access-list-log buffer

Displays ACL buffer characteristics.

Synopsis **show access-list-log buffer**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display buffer characteristics.

Usage Guidelines None

Examples None

See Also None

show ag

Displays the current Access Gateway configuration on a switch.

Synopsis `show ag [rbridge-id rbridge-id]`

Operands `rbridge-id rbridge-id` Specifies an RBridge ID for the switch.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display current, active configuration information for Access Gateway, such as the switch identification, number and type of ports, enabled policies, port grouping, and attached fabric details.

Usage Guidelines Consider these guidelines when automatic login balancing (lb) mode is enabled or disabled for a port group.

- When lb mode is disabled in a port group, the **show running-config ag**, **show ag map**, and **show ag** commands display the *configured* VF_Port to N_Port mapping. This is because configured and active mapping are the same.
- When LB mode is enabled in a port group, the **show ag** and **show ag map** commands display the *active* mapping only because VF_Port to N_Port mapping is based on the current distributed load across all N_Ports. The **show running-config ag** command displays the configured mapping only.

Examples Following is an example of the Access Gateway configuration on RBridge 5:

```
sw0# show ag
Rbridge-ID 5:
-----
Name           : sw0
NodeName       : 10:00:00:05:33:f4:78:04
Number of Ports : 32
IP Address(es) : 10.37.209.80
Firmware Version : v4.1.0pgoel_pit02_nos4_1_10_10
Number of N_Ports(Fi) : 2
Number of VF_Ports : 0
Policies Enabled : pg
Persistent ALPA  : Disabled
Port Group information :
  PG_ID  PG_Name PG_Mode PG_Members
  -----
  0      pg0     lb      5/0/1, 5/0/2, 5/0/3, 5/0/4,
                        5/0/5, 5/0/6, 5/0/7, 5/0/8
  -----

Fabric Information :
  Attached Fabric Name      N_Ports(Fi)
  -----
  10:00:00:05:33:72:f5:5a   5/0/1, 5/0/2

N_Port(Fi) information :
  Port      PortID      Attached PWWN      IP_Addr      VF_Ports
  -----
  Fi 5/0/1   0x020200   20:02:00:05:33:72:f5:5a   10.37.209.86   None
```

```
Fi 5/0/2      0x020300  20:03:00:05:33:72:f5:5a  10.37.209.86  None
-----
VF_Port information :
VF_Port  Eth_Port      PortID      Attached PWWN      N_Port(Fi)
-----
None
-----
```

See Also **show ag map, show running-config ag**

show ag map

Displays the current VF_Port mapping to N_Ports in Access Gateway mode on a specific switch or on all switches in the VCS cluster.

Synopsis `show ag map nport [rbridge-id {rbridge-id | all }]`

Operands `nport` N_Port number supported by the switch model in /rbridge-id/port group/N_Port format.

rbridge-id `rbridge-id` Specifies an RBridge ID for the switch.

all Specifies all RBridges in the VCS cluster.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current VF_Port to N_Port mapping on a local switch, a specific switch in the VCS cluster, or all switches in the cluster.

Usage Guidelines To display VF_Ports currently mapped to N_Ports on a specific switch, enter **show ag map rbridge-id rbridge-id**.

To display VF_Ports currently mapped to a specific N_Port on a specific switch, enter **show ag map nport rbridge-id rbridge-id**. In Network OS commands, N_Ports are designated by the format rbridge-id/port group/N_Port. Therefore, N_Port 5/0/1 designates that N_Port 1 resides in port group 0 on RBridge 5. The **show ag map** command for this N_Port would be the following:

```
show ag map 5/0/1 rbridge-id 5
```

To display VF_Ports currently mapped to a specific N_Port on all switches in the VCS cluster, enter **show ag map nport rbridge-id all**.

Consider these guidelines when Automatic Login Balancing (LB) mode is enabled or disabled for a port group.

- When Login Balancing (LB) mode is disabled in a port group, the **show running-config ag**, **show ag map**, and **show ag** commands display the *configured* VF_Port to N_Port mapping. This is because configured and active mapping are the same.
- When LB mode is enabled in a port group, **show ag** and **show ag map** commands display the *active* mapping only because VF_Port to N_Port mapping is based on the current distributed load across all N_Ports. The **show running-config ag** command displays the configured mapping only.

Examples Displaying port mapping information for a switch.

```
sw0# show ag map rbridge 5
```

```
Rbridge-ID 5:
```

```
-----
N_Port(Fi)    PG_ID  PG_Name  Current_VF_Ports
-----
5/0/1         0      pg0      None
5/0/2         0      pg0      None
5/0/3         0      pg0      None
5/0/4         0      pg0      None
5/0/5         0      pg0      None
5/0/6         0      pg0      None
```

5/0/7	0	pg0	None
5/0/8	0	pg0	None

See Also **map fport interface fcoe**

show ag pg

Displays information on Port Grouping (PG) configured on a switch for Access Gateway (AG) mode.

Synopsis	show ag pg [rbridge-id {rbridge-id all }]		
Operands	rbridge-id rbridge id	Specifies an RBridge ID for the switch.	
	all	Specifies all switches in the VCS cluster enabled for AG mode.	
Defaults	None		
Command Modes	Privileged EXEC mode		
Description	Use this command to display information on N_Port groups configured on a switch. This information includes N_Ports and VF_Ports in the group and Port Grouping (PG) modes enabled.		
Usage Guidelines	Access Gateway mode must be enabled.		
Examples	Following is an example showing port grouping information for RBridge 5:		

```
sw0# show ag pg rbridge-id 5
Rbridge-ID 5:
-----
PG_ID  PG_Name PG_Mode  N_Ports(Fi)                VF_Ports
-----
    0   pg0    1b      5/0/1,5/0/2,5/0/3,5/0/4, 1/5/1, 1/5/2, 1/5/3, 1/5/4,
                    5/0/5,5/0/6,5/0/7,5/0/8 1/5/5, 1/5/6, 1/5/7, 1/5/8,
                                      1/5/9, 1/5/10, 1/5/11, 1/5/12,
                                      1/5/13, 1/5/14, 1/5/15, 1/5/16,
                                      1/5/17, 1/5/18, 1/5/19, 1/5/20,
                                      1/5/21, 1/5/22, 1/5/23, 1/5/24,
                                      1/5/25, 1/5/26, 1/5/27, 1/5/28,
                                      1/5/29, 1/5/30, 1/5/31, 1/5/32,
                                      1/5/33, 1/5/34, 1/5/35, 1/5/36,
                                      1/5/37, 1/5/38, 1/5/39, 1/5/40,
                                      1/5/41, 1/5/42, 1/5/43, 1/5/44,
                                      1/5/45, 1/5/46, 1/5/47, 1/5/48,
                                      1/5/49, 1/5/50, 1/5/51, 1/5/52,
                                      1/5/53, 1/5/54, 1/5/55, 1/5/56,
                                      1/5/57, 1/5/58, 1/5/59, 1/5/60,
                                      1/5/61, 1/5/62, 1/5/63, 1/5/64
-----
```

See Also pg

show arp

Displays the ARP cache.

Synopsis **show arp** [[*switch_ID* | **all** | **dynamic** | **fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **ip** *ip-address* | **mac** | **slot** | **static** | **summary** | **tengigabitethernet** *rbridge-id/slot/port* | **ve** *vlan_id* | **vrf** *name*]]

Operands

<i>switch_ID</i>	Unique identifier for a switch (WWN).
all	Displays ARP information for all RBridge IDs in a cluster.
dynamic	Displays all the dynamic ARP entries in the ARP table.
fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
ip	Displays the ARP for a particular next-hop.
<i>ip-address</i>	Displays the ARP information for this next-hop IP address.
mac	Displays MAC-related ARP information.
slot	Displays ARP information for a selected slot.
static	Displays all the static ARP entries in the ARP table.
summary	Displays a summary of the ARP table (can be used by itself, or succeed the static, dynamic or interface keywords).
tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid external 10-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
ve <i>vlan_id</i>	Specifies the virtual Ethernet (VE) interface to display. Refer to the Usage Guidelines.
vrf <i>name</i>	Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

Defaults None

Command Modes Privileged EXEC mode

2 show arp

Description Use this command to display the contents of the ARP cache.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also None

show bpdu-drop

Displays information about BPDU guard.

Synopsis **show bpdu-drop** [**interface** {**port-channel** *num* | **fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port*]

Operands

interface	Selects an interface (required).
port-channel <i>num</i>	Selects a port channel interface. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
fortygigabitethernet	Selects a 40-GbE interface.
gigabitethernet	Selects a 1-GbE interface.
tengigabitethernet	Selects a 10-GbE interface.
<i>rbridge-id/slot/port</i>	Selects the RBridge ID, slot, and port of the respective interface.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about BPDU Guard.

Usage Guidelines This command is supported in VCS and standalone mode. This command can be entered on any RBridge in a Brocade VCS Fabric.

Examples None

See Also **capture packet interface**

show capture packet interface

Displays information about captured packets.

Synopsis **show capture packet interface** {**all** | **fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port*}

Operands

all	Selects all interfaces.
fortygigabitethernet	Selects a 40-GbE interface.
gigabitethernet	Selects a 1-GbE interface.
tengigabitethernet	Selects a 10-GbE interface.
<i>rbridge-id/slot/port</i>	Selects the RBridge ID, slot, and port of the respective interface.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information captured by means of the **capture packet interface** command.

Usage Guidelines This command is supported in VCS and standalone mode. This command can be entered on any RBridge in a Brocade VCS Fabric.

Examples

```
switch# show capture packet interface all
Packet Capture configured on the following interfaces
Te 130/0/5 >> ISL
Te 130/0/6 >> ISL
Te 130/0/21
Te 130/0/23
Te 130/0/24
```

```
Frame Received Time : Sat Mar 9 2013 0:57:0:282
Packet Type         : ELD
Packet Direction    : TX
Interface info       : Te 130/0/21
  ETHERNET HEADER
SrcMAC               : 00:05:33:5e:01:67
DstMAC               : 03:05:33:5d:f3:fa
Ethtype              : 0x8100
Eth Frametype        : 0x33
VlanID               : 0xffff
  ELD PAYLOAD DETAILS
-----
Vlan id              : 2
Src-Rbridgeid        : 130
Src-Priority          : 5
Magic Number         : 5103
```

See Also **capture packet interface**

show cee maps

Displays information on the defined CEE maps.

Synopsis **show cee maps default**

Operands None

Defaults The only map name allowed is “default.”

Command Modes Privileged EXEC mode

Description Use this command to display information on the CEE map. The configuration state is displayed with a list of all of the Layer 2 interfaces bound to the CEE map.

Usage Guidelines Network OS v4.1.0 only allows the CEE map named “default.”

Examples To view the CEE map:

```
switch0# show cee maps

CEE Map 'default'
  Precedence: 1
  Remap Fabric-Priority to Priority 0
  Remap Lossless-Priority to Priority 0
  Priority Group Table
    1: Weight 40, PFC Enabled, BW% 40
    2: Weight 40, PFC Disabled, BW% 40
    3: Weight 20, PFC Disabled, BW% 20
    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      3      1      2      2      2 15.0
```

See Also **cee, cee-map (configuration)**

show cert-util ldapca

Displays the LDAP Certification Authority (CA) certificate.

Synopsis `show cert-util ldapca [rbridge-id {rbridge_id | all}]`

Operands `rbridge-id rbridge-id` Specifies an RBridge ID for the switch.
`all` Specifies all switches in the VCS cluster.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the Lightweight Directory Access Protocol (LDAP) Certification Authority (CA) certificate.

Usage Guidelines None

Examples Standalone mode

To display the LDAP certificate on the switch:

```
switch# show cert-util ldapca
LDAP CA
```

VCS mode

To display the LDAP certificate on the switch:

```
switch: show cert-util syslogcacert rbridge-id 3
```

See Also ldap-server host, ldap-server maprole, show running-config ldap-server, username

show cert-util sshkey

Displays the public SSH key.

Synopsis **show cert-util sshkey user** *user_id* [**rbridge-id** {*rbridge-id* | **all** }]

Operands **user** *user_id* The user ID to display.
 rbridge-id *rbridge-id* Specifies an RBridge ID for the switch.
 all Specifies all switches in the VCS cluster.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the public SSH key for the user specified.

Usage Guidelines None

Examples Standalone mode

A typical output of this command:

```
switch# show cert-util sshkey user testuser
user's public keys
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAQEAtTCFzC1lfjwV9hjdTqv2ulSvmsmf7q7MS92Ctc3pDje/YGYJPHVU
i8bQX0XAsCAuzdsZL0BlVHdYPO1L4HStuIo8okfn4xLxrazqzwVeeL8p5Zcspf9zK8HmDzNpZ/OuQ9Mv
fOuzbseYrovqgYLFgfPvY6vleFXZo6lvVncFM7uFzasED9o9JUSBRORhBki7vB0SG69yNn6ADnmpQW6Q
Ou+nYuZaWXO0QXk2OIB+hidjxSQVAfVLidSIGyfDD0go+JAE3osxZxwQa5jcorASs4q2Gt4tSYERpvzO
sjaAR5YivbmmBTIQWdUuR9Laz8s8VKF4Di9HQ4kE+xyBeAFNvQ== bmeenaks@blc-10-6
```

VCS mode

To see the output of rbridge-id 3:

```
switch# show cert-util sshkey user testuser rbridge-id 3
```

See Also certutil import sshkey

show cert-util syslogca

Displays the syslog Certification Authority (CA) certificate.

Synopsis **show cert-util syslogca** [**rbridge-id** {*rbridge_id* | **all** }]

Operands **rbridge-id** *rbridge-id* Specifies an RBridge ID for the switch.
 all Specifies all switches in the VCS cluster.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the syslog 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*]

Operands **rbridge-id** *rbridge-id* Specifies an RBridge ID for the switch.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the Field Replaceable Unit (FRU) header content for each object in the chassis. Use this command to display the following information per line:

- Chassis name and model, for example, BR-VDX6720-24.
- The chassis backplane revision.
- 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.
- Object number: Slot number (for blades), Unit number (for everything else).
- If the FRU is part of an assembly, a brief description displays in parentheses.
- FRU header version number (Header Version: x) or blade version.
- The object's maximum allowed power consumption: a positive value for power supplies and a negative value for consumers. Power Consume Factor: -xxx.
- 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:
- Part number (up to 14 characters): Factory Part Num: xx-xxxxxx-x x
- Serial number (up to 12 characters): Factory Serial Num: xxxxxxxxxx
- FRU manufacture date: Manufacture: Day: *dd* Month: *mm* Year: *yyyy*
- Date of the last FRU header update: Update: Day: *dd* Month: *mm* Year: *yyyy*
- Cumulative time, in days, that the FRU has been inserted in the chassis with Network OS running: Time Alive :*dd* days
- Current time, in days, since the FRU was last powered on or the system was restarted: Time Awake: *dd* days
- Airflow direction (Brocade VDX 6710, 6720, 6730).
- Externally supplied ID (up to 10 characters): ID: xxxxxxxxxx
- Externally supplied part number (up to 20 characters): Part Num: xxxxxxxxxxxxxxxxxxxx
- Externally supplied serial number (up to 20 characters): Serial Num: xxxxxxxxxxxxxxxxxxxx
- Externally supplied revision number (up to 4 characters): Revision Num: xxxx

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

Pagination is not supported with this command. Use the “more” parameter to display the output one page at a time.

2 show chassis

Examples To display the FRU information on a Brocade VDX 6720-24:

```
switch# show chassis rbridge-id 9

Chassis Family:          BR-VDX6720-24
Chassis Backplane Revision: 2

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:          BR-VDX8770-4
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
```

2 show chassis

```
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 cipheraset

Displays the current cipheraset status.

Synopsis **show cipheraset**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current cipheraset status for LDAP and SSH.

Usage Guidelines None

Examples To display cipheraset status on the switch:

```
switch# show cipheraset  
LDAP Cipher List                : !DH:HIGH:-MD5  
SSH Cipher List                 : 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc
```

See Also **cipheraset**

show class-maps

Displays all the class-maps configured in the system.

Synopsis **show class-maps**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display all the class-maps configured in the system.

Usage Guidelines None

Examples None

See Also **class-map, policy-map**

show cli

Displays all the current CLI settings.

Synopsis **show cli**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display all the current CLI settings.

Usage Guidelines None

Examples Typical command output display.

```
switch# show cli
autowizard                false
complete-on-space        false
history                   100
idle-timeout              600
ignore-leading-space      false
output-file               terminal
paginate                  true
prompt1                   \H\M#
prompt2                   \H(\m)#
screen-length             73
screen-width              120
service prompt config    true
show-defaults             false
terminal                  ansi
```

See Also None

2 show cli history

show cli history

Displays the last 512 commands executed.

Synopsis **show cli history**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the last 512 commands executed on the local node across user sessions.

Usage Guidelines None

Examples None

See Also None

show clock

Returns the local time, date, and time zone.

Synopsis **show clock** [**rbridge-id** {*rbridge-id* | **all** }]

Operands **rbridge-id** *rbridge-id* Specifies an RBridge ID for the switch

all Specifies all switches in the VCS cluster.

Defaults The local clock is used.

Command Modes Privileged EXEC mode

Description Use this command to display the current local clock and time zone.

If the RBridge ID is not provided, status results default to the local switch (LOCL). If **rbridge-id all** is executed, the command displays the status for all switches in the VCS cluster.

Usage Guidelines This command is currently supported only on the local RBridge.

Examples Stand Alone mode

To show the local switch clock time:

```
switch# show clock
rbridge-id 1: 2012-05-04 16:01:51 Etc/GMT+0
```

VCS mode

To show clock time for all switches in the cluster (Logical chassis cluster mode only):

```
switch# show clock rbridge-id all
```

To show clock time for switch with rbridge-id 16:

```
switch# show clock rbridge-id 16
```

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

show config snapshot

Displays the snapshots present on the switch.

Synopsis **show config snapshot** [**rbridge-id** {*rbridge-id* | **all** }] [*snapshot-id*]

Operands	all	Displays all snapshot information.
	<i>rbridge-id</i>	Displays snapshots for the specified RBridge.
	<i>snapshot-id</i>	Specifies the name of the snapshot that has been captured. This can be any combination of characters and numbers. The range is from 1 through 50.

Defaults This command has no defaults.

Command Modes Privileged EXEC mode

Description Use this command to display the snapshots present on the switch.

Usage Guidelines A maximum of four snapshots for each RBridge ID can be stored on the switch.

Examples None

See Also **copy snapshot (logical chassis cluster mode)**

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	Specifies an RBridge ID for the switch.																										
	all	Specifies all switches in the VCS cluster.																										
Defaults	None																											
Command Modes	Privileged EXEC mode																											
Description	Use this command to display the status of the copy support operation on the local switch. The status is indicated by the percentage of completion. On a modular chassis, Use this command to display 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:																											
	<pre>switch# show copy-support status</pre> <table><thead><tr><th>Slot Name</th><th>SS type</th><th>Completion Percentage</th></tr></thead><tbody><tr><td>M1</td><td>NORMAL</td><td>[100%]</td></tr><tr><td>M2</td><td>NORMAL</td><td>[100%]</td></tr><tr><td>L1/0</td><td>NORMAL</td><td>[100%]</td></tr><tr><td>L1/1</td><td>NORMAL</td><td>[100%]</td></tr><tr><td>L2/0</td><td>NORMAL</td><td>[100%]</td></tr><tr><td>L2/1</td><td>NORMAL</td><td>[100%]</td></tr><tr><td>L4/0</td><td>NORMAL</td><td>[100%]</td></tr><tr><td>L4/1</td><td>NORMAL</td><td>[100%]</td></tr></tbody></table>		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
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 dadstatus

Displays the current DHCP auto-deployment (DAD) status output on the switch.

Synopsis **show dadstatus**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the DAD status output on the switch.

Usage Guidelines If DAD fails, one of the following errors will show in the output:

1. DHCP auto-deployment failed during DHCP process
2. DHCP auto-deployment failed in sanity check
3. DHCP auto-deployment failed due to same firmware
4. DHCP auto-deployment failed to start firmware download
5. DHCP auto-deployment failed due to firmware download failure

Examples To display DAD status output on the switch:

```
sw0# show dadstatus
[1] : Thu Aug 15 23:22:50 GMT 2013
DHCP Auto-deployment enabled

[2] : Thu Aug 15 23:27:20 GMT 2013
DHCP Auto-deployment started firmwaredownload

[3] : Thu Aug 15 23:38:57 GMT 2013
DHCP Auto-deployment succeeded

sw0# show dadstatus
[1] : Fri Aug 16 12:02:44 GMT 2013
DHCP Auto-deployment enabled

[2] : Fri Aug 16 12:10:03 GMT 2013
DHCP Auto-deployment failed in sanity check.
```

See Also firmware download, firmware download logical-chassis, dhcp auto-deployment enable

show debug dhcp packet

Displays the DHCP packet capture configuration for interfaces configured for DHCP packet capturing.

Synopsis **show debug dhcp packet**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Displays the DHCP packet capture configuration for each interface configured for DHCP packet capture.

Usage Guidelines None

Examples sw0# **show debug dhcp packet**
% DHCP protocol RCV debug is enabled on interface Te 3/18
% DHCP protocol TX debug is enabled on interface Te 3/18
PCAP Buffer Configuration for Vrf ID 0: Buffer Type is Linear and BufferSize is 2056

See Also **debug dhcp packet buffer interface**

show debug dhcp packet buffer

Displays DHCP packets saved in the DHCP packet capture buffer.

Synopsis	show debug dhcp packet buffer
Operands	None
Defaults	None
Command Modes	Privileged EXEC mode
Description	This command displays DHCP capture buffer content for all VRF IDs.
Usage Guidelines	None
Examples	The following command displays buffer content for all VRF IDs.

```
sw0# show debug dhcp packet buffer
Protocol Type      : DHCP
Packet Flow       : RX
Src Port          : 68 (DHCP Client)
Dst Port          : 67 (DHCP Server)
Message Type      : 1 (DHCP-Discover)
Hardware Type     : 1 (Ethernet (10Mb))
Hw Address Len    : 6
Hops              : 0
Transaction ID     : 0
Seconds Elapsed   : 0
BootP Flags       : 8000
Client IP         : 0.0.0.0
Your (client) IP  : 0.0.0.0
Next Server IP    : 0.0.0.0
Relay Agent IP    : 0.0.0.0
Client MAC Add    : 00:10:94:00:00:01
Server Host Name  : Not Given
Boot File Name    : Not Given
*****
```

```
Protocol Type      : DHCP
Packet Flow       : TX
Src Port          : 67 (DHCP Server)
Dst Port          : 68 (DHCP Client)
Message Type      : 2 (DHCP-Offer)
Hardware Type     : 1 (Ethernet (10Mb))
Hw Address Len    : 6
Hops              : 1
Transaction ID     : 0
Seconds Elapsed   : 0
BootP Flags       : 8000
Client IP         : 0.0.0.0
Your (client) IP  : 10.10.10.30
Next Server IP    : 20.20.20.20
Relay Agent IP    : 10.10.10.10
Client MAC Add    : 00:10:94:00:00:01
Server Host Name  : Not Given
Boot File Name    : Not Given
*****
```

```
Protocol Type      : DHCP
Packet Flow       : RX
Src Port          : 68 (DHCP Client)
Dst Port          : 67 (DHCP Server)
Message Type      : 3 (DHCP-Request)
Hardware Type     : 1 (Ethernet (10Mb))
Hw Address Len    : 6
Hops              : 0
Transaction ID    : 0
Seconds Elapsed   : 0
BootP Flags       : 8000
Client IP         : 0.0.0.0
Your (client) IP  : 0.0.0.0
Next Server IP    : 0.0.0.0
Relay Agent IP    : 0.0.0.0
Client MAC Add    : 00:10:94:00:00:01
Server Host Name  : Not Given
Boot File Name    : Not Given
*****
```

```
Protocol Type      : DHCP
Packet Flow       : TX
Src Port          : 67 (DHCP Server)
Dst Port          : 68 (DHCP Client)
Message Type      : 5 (DHCP-Ack)
Hardware Type     : 1 (Ethernet (10Mb))
Hw Address Len    : 6
Hops              : 1
Transaction ID    : 0
Seconds Elapsed   : 0
BootP Flags       : 8000
Client IP         : 0.0.0.0
Your (client) IP  : 10.10.10.30
Next Server IP    : 20.20.20.20
Relay Agent IP    : 10.10.10.10
Client MAC Add    : 00:10:94:00:00:01
Server Host Name  : Not Given
Boot File Name    : Not Given
*****
```

See Also **debug dhcp packet buffer interface, debug dhcp packet buffer clear**

2 show debug ip bgp all

show debug ip bgp all

Displays all BGP4 debug options that are enabled.

Synopsis **show debug ip bgp all**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view all BGP4 debug options that are enabled.

Usage Guidelines None

Examples switch# **show debug ip bgp all**

See Also None

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 Use this command to display the IGMP packets received and transmitted.

Usage Guidelines None

Examples None

See Also None

2 show debug ip pim

show debug ip pim

Displays the current state of the Protocol Independent Multicast (PIM) debug flags.

Synopsis **show debug ip pim**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the status of PIM debugging flags on the switch.

Usage Guidelines None

Examples A typical output of this command.

```
switch# show debug ip pim
PIM debugging status:
-----
add-del-oif   : off
bootstrap    : off
group         : off
join-prune    : on
nbr-change    : off
packets       : off
parent        : off
regproc       : off
route-change  : off
rp            : off
source        : off
-----
```

See Also None

show debug lacp

Displays the configured debugging features for LACP.

Synopsis **show debug lacp**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the status of LACP debugging flags on the switch.

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 status of LLDP debugging flags 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 status of STP debugging flags on the switch.

Usage Guidelines None

Examples None

See Also None

show debug udd

Shows UDLD debug status on the switch.

Synopsis **show debug udd**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to show the unidirectional link detection (UDLD) protocol debug status of the switch. The status reflects the bugging you set with the **debug udd** command.

Usage Guidelines None

Examples To display the debug status of the switch:

```
switch# show debug udd  
Interface TenGigabitEthernet 5/0/3 : None  
Interface TenGigabitEthernet 5/0/2 : Transmit and Receive  
Interface TenGigabitEthernet 5/0/1 : Transmit
```

See Also **protocol udd, debug udd**

show debug vrrp

Displays debug parameters.

Synopsis **show debug vrrp**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the status of VRRP debugging flags on the switch.

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 parameter has already been set to debug all VRRP events, the following is displayed:

```
switch# show debug vrrp  
VRRP event debugging is on
```

See Also None

show defaults threshold

Displays the default thresholds for environmental and alert values for Ethernet interfaces, security monitoring, and SFPs.

Synopsis	show defaults threshold [interface type Ethernet security sfp]
Operands	interface type Ethernet Thresholds for all Ethernet interfaces. security Thresholds for login and Telnet monitoring. sfp Thresholds for the following SFP types: 1 GLR 1 GSR 10 GLR 10 GSR 10 GUSR QSFP
Defaults	None
Command Modes	Privileged EXEC mode
Description	Use this command to display default thresholds for environmental and alert values for Ethernet interfaces, login and Telnet security, and SFPs. These thresholds can be changed by means of the threshold-monitor command.
Usage Guidelines	None
Examples	The following example illustrates default interface thresholds:

switch# **show defaults threshold interface type Ethernet**

Type: GigE-Port

Area	High Threshold			Low Threshold			Buffer Value	Time Base
	Value	Above Action	Below Action	Value	Above Action	Below Action		
MTC	300	none	none	12	none	none	0	minute
CRCAlign	300	none	none	12	none	none	0	minute
Symbol	5	none	none	0	none	none	0	minute
IFG	100	none	none	5	none	none	0	minute

MTC - Missing Termination Character

The following example illustrates security thresholds:

```
sw0# show defaults threshold security
```

Area	High Threshold			Low Threshold		Buffer	Time
	Value	Above Action	Below Action	Value	Below Action	Value	Base
Telnet	2	raslog	none	1	none	0	minute
Login	2	raslog	none	1	none	0	minute

See Also **show threshold monitor, threshold-monitor cpu**

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 dpod

Displays Dynamic Ports on Demand (DPoD) licensing.

Synopsis **show dpod** [**rbridge-id** {*rbridge-id* | **all**}]

Operands **rbridge-id** *rbridge-id* Specifies an RBridge ID for the switch.
all Specifies all RBridge IDs in the VCS cluster.

Defaults None

Current 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 Brocade VDX 6710 and VDX 8770 switches. These switches do not support the Dynamic POD feature.

In logical chassis cluster mode, remote license operations may be performed on any remote RBridge, from any RBridge in the logical chassis cluster.

Examples

```
switch# show dpod
rbridge-id: 15
  48 10G ports are available in this switch
    4 40G ports are available in this switch
    10G Port Upgrade license is installed
    40G Port Upgrade license is installed
    Dynamic POD method is in use

  32 10G port assignments are provisioned for use in this switch:
    24 10G port assignments are provisioned by the base switch license
      8 10G port assignments are provisioned by the Port Upgrade license
    1 10G port is assigned to installed licenses:
      1 10G port is assigned to the base switch license
      0 10G ports are assigned to the Port Upgrade license
  10G ports assigned to the base switch license:
    15/0/12
  10G ports assigned to the Port Upgrade license:
    None
  10G ports not assigned to a license:
    15/0/1, 15/0/2, 15/0/3, 15/0/4, 15/0/5, 15/0/6, 15/0/7, 15/0/8, 15/0/9,
  15/0/10
    15/0/11, 15/0/13, 15/0/14, 15/0/15, 15/0/16, 15/0/17, 15/0/18, 15/0/19,
  15/0/20, 15/0/21
    15/0/22, 15/0/23, 15/0/24, 15/0/25, 15/0/26, 15/0/27, 15/0/28, 15/0/29,
  15/0/30, 15/0/31
    15/0/32, 15/0/33, 15/0/34, 15/0/35, 15/0/36, 15/0/37, 15/0/38, 15/0/39,
  15/0/40, 15/0/41
    15/0/42, 15/0/43, 15/0/44, 15/0/45, 15/0/46, 15/0/47, 15/0/48
  31 10G license reservations are still available for use by unassigned ports

  16 40G port assignments are provisioned for use in this switch:
    0 40G port assignments are provisioned by the base switch license
    2 40G port assignments are provisioned by the Port Upgrade license
  1 40G port is assigned to installed licenses:
    0 40G ports are assigned to the base switch license
```

2 show dpod

```
      1 40G ports are assigned to the Port Upgrade license
40G ports assigned to the base switch license:
      None
40G ports assigned to the Port Upgrade license:
      15/0/49
40G ports not assigned to a license:
      15/0/50, 15/0/51, 15/0/52
      3 40G license reservations are still available for use by unassigned ports

switch#
```

See Also **show running-config dpod**

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** *rbridge-id*]

Operands **rbridge-id** *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 [slot slot-id]	
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 nonvolatile storage memory in the switch.

- Synopsis

show diag burninstatus [**rbridge-id** *rbridge-id*]
- Operands

rbridge-id *rbridge-id* Specifies the RBridge ID for the switch.
- 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** *rbridge-id*] [**slot** *slot-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.

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 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 prbctest 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)
```

2 show diag post results

`rbridgeId 1`

See Also **diag post enable**

show diag setcycle

Displays the current systemVerification test parameters.

Synopsis **show diag setcycle** [**rbridge-id** *rbridge-id*]

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID of the switch.

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** *rbridge-id*] [**slot** *slot-id*]

Operands **rbridge-id***rbridge-id* Specifies the RBridge ID of the switch to display.
 slot *slot_id* Specifies the slot ID. This is mandatory for slot-based systems only.

Defaults If an RBridge ID is not specified, diagnostic tests for all blades in the system are displayed.

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

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the 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 all diagnostics information for the authenticator associated with a port.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

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
authEaploggogWhileAuthenticating: 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** *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the 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 state of a specified interface.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display the state of the 10-gigabit 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** *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the 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 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	<i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
		<i>rbridge-id</i>	Specifies the RBridge ID.
		<i>slot</i>	Specifies a valid slot number.
		<i>port</i>	Specifies a valid port number.
	gigabitethernet	<i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
		<i>rbridge-id</i>	Specifies the RBridge ID.
		<i>slot</i>	Specifies a valid slot number.
		<i>port</i>	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** parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display the statistics for the 10-gigabit 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** *rbridge-id* | **all**]

Operands **rbridge-id** *rbridge-id* Specifies an RBridge ID for the switch.
all Specifies all switches in the VCS 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 Brocade VDX 6710 or VDX 8770 switches.
 In the Network OS v3.0.0 release Use this command to display 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 detail

Displays ELD detailed information for the entire node.

Synopsis **show edge-loop-detection detail** [**rbridge-id** {*rbridge-id* | **all**}]

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID.
all Specifies all RBridge IDs in the VCS cluster.

Defaults None

Command Modes Privileged EXEC mode
ELD configuration mode

Description Use this command to view detailed ELD information for the entire node.

Usage Guidelines This functionality detects Layer 2 loops only.

If no **rbridge-id** *rbridge-id* is specified, ELD data on the particular node is displayed.

If **rbridge-id** *rbridge-id* is specified, ELD data for the node with that particular rbridge-id is displayed.

If **rbridge-id** **all** is specified, ELD data from all the nodes in the cluster is displayed.

Examples `switch(conf-if-te-119/0/1)# do show edge-loop-detection detail`

Number of edge-loop-detection instances enabled: 1

```
Data for Rbridge-id: 119
Total_instances: 1
Eld-mac: 03:05:33:65:1b:ec
```

```
Data for interface: te0/1
Eld-instance no. (enabled for VLANs): 1
Priority: 128   If_status: 1
Shutdown-vlan: 0      Vlag-master-id: 0      Age-left: 31913 mins
Port-type : 3   pvid_frame_type: 2      Brcd-agg-type: 0
Eld stats:      Tx      Rx
                42      0
Enabled for Vlan-id: 10
Send-untagged: 0
time-rxlimit : 0
Vlan stats:      Tx      Rx
                42      0
```

```
switch(conf-if-te-119/0/1)#
```

See Also **edge-loop-detection vlan, hello-interval, pdu-rx-limit, protocol edge-loop-detection, shutdown-time**

show edge-loop-detection globals

Displays ELD global configuration values for status, disabled ports, and resource.

Synopsis **show edge-loop-detection globals**

Operands None

Defaults None

Command Modes Privileged EXEC mode
 ELD configuration 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** *interface-type interface-id*
show edge-loop-detection interface {**tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **port-channel** *number*}

Operands *interface-type* Specifies an interface type.
interface-id Specifies an interface ID.
tengigabitethernet *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface.
 rbridge-id Specifies the RBridge ID. This value 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-gigabit Ethernet interface.
 rbridge-id Specifies the RBridge ID. 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. Valid values range from 1 through 6144.

Defaults None

Command Modes Privileged EXEC mode
 ELD configuration 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 This functionality detects Layer 2 loops only.

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
```

```
switch(conf-if-te-7/0/5)# do 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, protocol edge-loop-detection, shutdown-time**

show edge-loop-detection rbridge-id

Displays ELD status information for a specific RBridge.

Synopsis **show edge-loop-detection rbridge-id** {*rbridge-id* | **all**}

Operands *rbridge-id* Specifies an RBridge ID for the switch.
all Specifies all RBridge IDs in the VCS cluster.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view the configuration and status of ELD on a specific RBridge, 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.

If **rbridge-id** *rbridge-id* is specified, ELD data for the node with that particular *rbridge-id* is displayed.

If **rbridge-id** **all** is specified, ELD data from all the nodes in the cluster is displayed.

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 RBridge ID. This parameter is not valid in standalone mode, and is supported only for the local RBridge ID.

all Specifies all switches in the fabric. This parameter 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” parameter 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 RBridge ID. This parameter is not valid in standalone mode, and is supported only for the local RBridge ID.

all Specifies all switches in the fabric. This parameter 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-yyyyyy-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” parameter 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 RBridge ID. This parameter is not valid in standalone mode, and is supported only for the local RBridge ID.

all Specifies all switches in the fabric. This parameter 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 RBridge ID. This parameter is not valid in standalone mode, and is supported only for the local RBridge ID.

all Specifies all switches in the fabric. This parameter 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 RBridge ID. This parameter is not valid in standalone mode, and is supported only for the local RBridge ID.	
	all	Specifies all switches in the fabric. This parameter 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, Use this command to display 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:		
	<pre>switch# show environment temp Sensor State Centigrade Fahrenheit ID ===== 1 Ok 36 96 2 Ok 40 104 3 Ok 32 89</pre>		
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 reconfiguring, 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 or same-level RBridge.

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

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* Specifies the RBridge ID

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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.

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Examples Some typical outputs of this 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 RBridge ID. 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:

<i>Rbridge-id</i>	RBridge-id of the switch. Valid values range from 1 through 239.
<i>#ISLs</i>	Number of ISLs connected.
<i>Src Index</i>	Source index of the local RBridge.
<i>Src Interface</i>	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.
<i>Nbr Index</i>	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.
<i>Nbr Interface</i>	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 “?/?/?”.
<i>Nbr-WWN</i>	Neighbor WWN of the switch. If the ISL is segmented and the neighbor RBridge details are not available, then “?:?:?:?:?:?:?:?:?:?” displays in this field.
<i>BW</i>	Bandwidth of the traffic.
<i>Trunk</i>	Displays “Yes” if trunk is enabled in the ISL.
<i>Nbr-Name</i>	Neighbor switch name.

Usage Guidelines This command is not available in standalone mode.

If this command is executed without operands, the output displays the ISL information of the local RBridge.

The **show fabric** family of commands displays 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.

2 show fabric isl

When a switch in a fabric is running Network OS 4.0.1 or later, CLI output displays the QSFP breakout index information for those switches, which includes the port followed by a colon (:) and the breakout indicator.

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Examples This example displays Inter-Switch Link (ISL) information in the fabric.

```
switch# show fabric isl
Rbridge-id: 76 #ISLs: 2
```

Src Index	Src Interface	Nbr Index	Nbr 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"

This example displays ISL information and includes a segmented link.

```
switch# show fabric isl
Rbridge-id: 2 #ISLs: 4
```

Src Index	Src Interface	Nbr Index	Nbr 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"

This example displays ISL information and includes an Fi port.

```
switch# show fabric isl
Rbridge-id: 66 #ISLs: 5
```

Src Index	Src Interface	Nbr Index	Nbr 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"

This ISL output example includes breakout information for switches on which breakout mode is configured.

```
switch# show fabric isl
Rbridge-id: 66 #ISLs: 5
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr-WWN	BW	Trunk	Nbr-Name
5	Te 66/0/5:1	1	Te 65/0/1	10:00:00:05:33:5F:EA:A4	10G	Yes	"sw0"
15	Te 66/0/15	2	Te 65/0/2:1	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 66/0/35:1	4	Te 65/0/4:4	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"

This example displays ISL details and includes the breakout index of the interface (for a non-trunked port) in normal mode.

```
switch# sh fab isl
```

```
Rbridge-id: 1    #ISLs: 4
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr-WWN	BW	Trunk	Nbr-Name
30	Te 1/0/27	1	Te 48/0/49:1	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "
32	Te 1/0/29	2	Te 48/0/49:2	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "
34	Te 1/0/31	3	Te 48/0/49:3	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "
36	Te 1/0/33	4	Te 48/0/49:4	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "

This example displays ISL details and includes the breakout index of the interface (for a trunked port) in normal mode.

```
switch# sh fab isl
```

```
Rbridge-id: 1    #ISLs: 1
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr-WWN	BW	Trunk	Nbr-Name
5	Te 1/0/50:1	1	Te 48/0/49:1	10:00:00:05:33:E5:C1:8F	40G	Yes	"sw0 "

This example displays ISL details in mixed mode, but no breakout index is displayed for switches running Network OS versions earlier than v4.1.0.

Output shown is for Network OS 4.0.0 for a non-trunked port in mixed mode.

```
sw0# sh fab isl
```

```
Rbridge-id: 1    #ISLs: 4
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr-WWN	BW	Trunk	Nbr-Name
30	Te 1/0/27	1	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "
32	Te 1/0/29	1	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "
34	Te 1/0/31	1	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "
36	Te 1/0/33	1	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "

Output shown is for Network OS 4.0.0 for a trunked port in mixed mode.

```
sw0# sh fab isl
```

```
Rbridge-id: 1    #ISLs: 1
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr-WWN	BW	Trunk	Nbr-Name
2	Te 1/0/50	1	Te 48/0/49	10:00:00:05:33:E5:C1:8F	40G	Yes	"sw0 "

Output shown is for Network OS 4.1.0 for a non-trunked port in mixed mode.

```
sw0# sh fab isl
```

```
Rbridge-id: 48    #ISLs: 4
```

2 show fabric isl

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr-WWN	BW	Trunk	Nbr-Name
1	Te 48/0/49:1	30	Te 1/0/25	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "
1	Te 48/0/49:2	32	Te 1/0/27	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "
1	Te 48/0/49:3	34	Te 1/0/29	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "
1	Te 48/0/49:4	36	Te 1/0/31	XX:XX:XX:XX:XX:XX:XX:XX	10G	Yes	"sw0 "

Output shown is for Network OS 4.1.0 for a trunked port in mixed mode.

```
sw0# sh fab isl
```

```
Rbridge-id: 1    #ISLs: 1
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr-WWN	BW	Trunk	Nbr-Name
30	Te 1/0/50:1	1	Te 48/0/49	10:00:00:05:33:E5:C1:8F	40G	Yes	"sw0 "

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 RBridge ID 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	VCS ID. Valid values range 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. Valid values range from 1 through 239.
WWN	Switch world wide name (WWN).
FCF MAC	Mac address
Index	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 of those listed below.

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 inc om pat ability	ECP rejected or retries exceeded.
11	FDS Zone Conflict	FDS configuration caused zone conflict.
12	ESC mismatch, VCS Virtual Fabric Mode Conflict	Virtual Fabric mode is enabled on one end and disabled on the other end.

In this command, disabled ports are denoted as “Down (Disabled reason)”. The disabled reason could be any of those listed below.

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 inc om pat ability	Long distance configuration doesn't match.
5	ELP retries exceeded	Max ELP retries 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.

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.

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Examples

To display information for all ISL ports in the core switch:

```
switch# show fabric islports
```

```
Name:          sw0
Type:          96.5
State:         Online
Role:          Fabric Principal
VCS Id:        1
Config Mode: Local-Only
Rbridge-id:    23
WWN:           10:00:00:05:33:d1:3a:ac
FCF MAC:       00:05:33:d1:3a:ac
```

```

Index  Interface      State  Operational State
=====
0      Fi 23/0/1       Up     ISL (protocol incomplete)
1      Fi 23/0/2       Up     F-Port
2      Fi 23/0/3       Up     F-Port
3      Fi 23/0/4       Up     F-Port
4      Fi 23/0/5       Up     Loopback-> Fi 23/0/5
5      Fi 23/0/6       Down
6      Fi 23/0/7       Down
7      Fi 23/0/8       Down
8      Te 23/0/1       Up     ISL segmented, (ESC mismatch, Config Mode) (Trunk Primary)
9      Te 23/0/2       Down
10     Te 23/0/3       Down
11     Te 23/0/4       Down
12     Te 23/0/5       Down
13     Te 23/0/6       Down
14     Te 23/0/7       Down
15     Te 23/0/8       Down
16     Te 23/0/9       Down
17     Te 23/0/10      Down
18     Te 23/0/11      Down
19     Te 23/0/12      Down
20     Te 23/0/13      Down
21     Te 23/0/14      Down
22     Te 23/0/15      Down
23     Te 23/0/16      Down
24     Te 23/0/17      Down
25     Te 23/0/18      Down
26     Te 23/0/19      Down
27     Te 23/0/20      Down
28     Te 23/0/21      Down
29     Te 23/0/22      Down
30     Te 23/0/23      Down
31     Te 23/0/24      Down

```

2 show fabric islports

See Also fabric isl enable, show diag burninstatus, show fabric isl, show fabric trunk

show fabric port-channel

Displays the fabric VLAG load-balance information.

Synopsis **show fabric port-channel** [*port-channel-id* | **load-balance**]

Operands *port-channel-id* Displays the information for the port channel ID.

load-balance Displays the load balance information.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the fabric's VLAG load-balance information.

Usage Guidelines This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Examples switch# **show fabric port-channel 10 load-balance**
Fabric Vlag Load-Balance Information

Port-channel id : 10
Load-Balance Flavor : Source and Destination MAC address and VID based load
balancing

See Also **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 Use this command to display details about all the links connected to the fabric. It groups the information for each RBridge in the fabric.

The command displays the following fields of information:

Rbridge-id	ID of the RBridge. Valid values range from 1 through 239.
Reachable	Indicates whether the RBridge 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 RBridge.
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.

The output displays the link information, which includes the breakout index of the interface if breakout mode is configured in the source or neighbor interface.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1.0.

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 Index	Src Interface	Nbr Index	Nbr 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 Index	Src Interface	Nbr Index	Nbr 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 Index	Src Interface	Nbr Index	Nbr 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 Index	Src Interface	Nbr Index	Nbr 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 Index	Src Interface	Nbr Index	Nbr 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	

2 show fabric route linkinfo

This example displays link linformation and includes the breakout index of the interface in normal mode.

```
sw0# show fabric route linkinfo
```

```
Rbridge-id: 1
=====
Reachable:    Yes
Version:      1
No. of Links: 4
Link#   Src      Src      Nbr      Nbr      Link-Cost  Link-Type  Trunk
      Index  Interface Index  Interface
-----
1       28       Te 1/0/49:1  0       Te 48/0/49:1  500       Pt_Pt Ethernet
2       30       Te 1/0/49:2  1       Te 48/0/49:2  500       Pt_Pt Ethernet
3       32       Te 1/0/49:3  2       Te 48/0/49:3  500       Pt_Pt Ethernet
4       34       Te 1/0/49:4  3       Te 48/0/49:4  500       Pt_Pt Ethernet
```

```
Rbridge-id: 48
=====
Reachable:    Yes
Version:      1
No. of Links: 4
Link#   Src      Src      Nbr      Nbr      Link-Cost  Link-Type  Trunk
      Index  Interface Index  Interface
-----
1       0       Te 48/0/49:1  28      Te 1/0/49:1  500       Pt_Pt Ethernet
2       1       Te 48/0/49:2  30      Te 1/0/49:2  500       Pt_Pt Ethernet
3       2       Te 48/0/49:3  32      Te 1/0/49:3  500       Pt_Pt Ethernet
4       3       Te 48/0/49:4  34      Te 1/0/49:4  500       Pt_Pt Ethernet
```

This example displays link linformation and includes the breakout index of the interface in mixed mode running Network OS v4.0.0:

```
switch# show fabric route linkinfo
```

```
Rbridge-id: 1
=====
Reachable:    Yes
Version:      1
No. of Links: 4
Link#   Src      Src      Nbr      Nbr      Link-Cost  Link-Type  Trunk
      Index  Interface Index  Interface
-----
1       28       Te 1/0/49  0       Te 48/0/49  500       Pt_Pt Ethernet
2       30       Te 1/0/49  1       Te 48/0/49  500       Pt_Pt Ethernet
3       32       Te 1/0/49  2       Te 48/0/49  500       Pt_Pt Ethernet
4       34       Te 1/0/49  3       Te 48/0/49  500       Pt_Pt Ethernet
```

```
Rbridge-id: 48
=====
Reachable:    Yes
Version:      1
No. of Links: 4
Link#   Src      Src      Nbr      Nbr      Link-Cost  Link-Type  Trunk
      Index  Interface Index  Interface
-----
1       0       Te 48/0/49  28      Te 1/0/49  500       Pt_Pt Ethernet
2       1       Te 48/0/49  30      Te 1/0/49  500       Pt_Pt Ethernet
3       2       Te 48/0/49  32      Te 1/0/49  500       Pt_Pt Ethernet
```

```

4          3          Te 48/0/49    34          Te 1/0/49          500          Pt_Pt Ethernet

```

This example displays link linformation and includes the breakout index of the interface in mixed mode running Network OS v4.1.0:

```
switch# show fabric route linkinfo
```

```

Rbridge-id: 1
=====
Reachable:    Yes
Version:      1
No. of Links: 4
Link#      Src      Src      Nbr      Nbr
  Index    Interface  Index    Interface  Link-Cost  Link-Type  Trunk
-----
1         28        Te 1/0/49:1    0        Te 48/0/49    500        Pt_Pt Ethernet
2         30        Te 1/0/49:2    1        Te 48/0/49    500        Pt_Pt Ethernet
3         32        Te 1/0/49:3    2        Te 48/0/49    500        Pt_Pt Ethernet
4         34        Te 1/0/49:4    3        Te 48/0/49    500        Pt_Pt Ethernet

```

```

Rbridge-id: 48
=====
Reachable:    Yes
Version:      1
No. of Links: 4
Link#      Src      Src      Nbr      Nbr
  Index    Interface  Index    Interface  Link-Cost  Link-Type  Trunk
-----
1         0         Te 48/0/49:1    28        Te 1/0/49    500        Pt_Pt Ethernet
2         1         Te 48/0/49:2    30        Te 1/0/49    500        Pt_Pt Ethernet
3         2         Te 48/0/49:3    32        Te 1/0/49    500        Pt_Pt Ethernet
4         3         Te 48/0/49:4    34        Te 1/0/49    500        Pt_Pt Ethernet

```

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 RBridge ID. 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. Valid values range from 1 through 239.
Mcast Priority	Mcast priority value of the switch. Valid values range 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 connected 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.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1.0. In such instances, the neighbor port WWN (Nbr-WWN) is displayed as XX:XX:XX:XX:XX:XX:XX:XX.

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

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

This example displays route information and includes the breakout index of the interface in normal mode.

```
sw0# show fabric route multicast
```

```

Root of the Multicast-Tree
=====
Rbridge-id: 1
Mcast Priority: 1
Enet IP Addr: 10.38.19.47
WWN: 10:00:00:05:33:65:0b:20
Name: sw0

```

```
Rbridge-id: 48
```

Src-Index	Src-Port	Nbr-Index	Nbr-Port	BW	Trunk
0	Te 48/0/49:1	28	Te 1/0/49:1	0G	

This example displays route information and includes the breakout index of the interface in mixed mode running Network OS v4.0.0.

```
sw0# show fabric route multicast
```

```

Root of the Multicast-Tree
=====
Rbridge-id: 1
Mcast Priority: 1
Enet IP Addr: 10.38.19.47
WWN: 10:00:00:05:33:65:0b:20
Name: sw0

```

```
Rbridge-id: 1
```

Src-Index	Src-Port	Nbr-Index	Nbr-Port	BW	Trunk
28	Te 1/0/49	0	Te 48/0/49	10G	

This example displays route information and includes the breakout index of the interface in mixed mode running Network OS v4.1.0.

```
sw0# show fabric route multicast
```

2 show fabric route multicast

```
Root of the Multicast-Tree
=====
Rbridge-id: 1
Mcast Priority: 1
Enet IP Addr: 10.38.19.47
WWN: 10:00:00:05:33:65:0b:20
Name: sw0
```

```
Rbridge-id: 1
```

Src-Index	Src-Port	Nbr-Index	Nbr-Port	BW	Trunk
0	Te 48/0/49:1	28	Te 1/0/49	10G	

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 RBridge ID of the RBridge for which neighbor information is to be displayed.

all Displays neighbor information for all RBridges in the fabric.

Defaults If no RBridge is specified, the neighbor state information for the local switch is displayed.

Command Modes Privileged EXEC mode

Description Use this command to display information about neighbors to a specified RBridge. FSPF defines a neighbor as a remote ISL interface that is directly attached to the local RBridge. 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 RBridge. Valid values range 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 <i>rbridge-id/slot/port</i> ". 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 <i>rbridge-id/slot/port</i> ". 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."

2 show fabric route neighbor-state

The **show fabric** family of commands display neighbor and local port information when connected to a down-level RBridge.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1.0. This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Examples To display the state of FSPF neighbors for the local switch:

```
switch# show fabric route neighbor-state
Rbridge-id: 66 #ISLs: 8
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr 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

This example displays neighbor state route details and includes the breakout index of the interface in normal mode.

```
sw0# show fabric route neighbor-state
```

```
Rbridge-id: 1 #ISLs: 1
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr State
30	Te 1/0/49:1	1	Te 48/0/49:1	NB_ST_FULL

This example displays neighbor state route details of the non-trunked port in mixed mode running Network OS v4.0.0. (In mixed mode, the QSFP breakout index is not displayed in the output on a switch running Network OS versions earlier than v4.1.0.)

```
sw0# show fabric route neighbor-state
```

```
Rbridge-id: 1 #ISLs: 2
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr State
30	Te 1/0/49	1	Te 48/0/49	NB_ST_FULL

This example displays neighbor state route details of the non-trunked port in mixed mode running Network OS v4.1.0.

```
sw0# show fabric route neighbor-state
```

```
Rbridge-id: 1 #ISLs: 2
```

Src Index	Src Interface	Nbr Index	Nbr Interface	Nbr State

30	Te 1/0/49:1	1	Te 48/0/49	NB_ST_FULL

See Also show fabric route topology, show fabric route linkinfo

show fabric route pathinfo

Displays the path of a data stream through a fabric and provides statistics about each hop on that path.

Synopsis **show fabric route pathinfo Fabric ID Domain Source Port Destination Port Basic Stats Extended Stats Reverse Path**

Operands You are prompted to select parameters interactively. The command will prompt 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 RBridge 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. 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, basic 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.

Defaults This command has no inherent defaults. Refer to the Description for parameter-specific defaults.

Command Modes Privileged EXEC mode

Description Use this command to display 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.

Regardless of parameter 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 1 second interval that the port was unable to transmit frames because the transmit BB credit was 0. The purpose of this statistic is to detect congestion or a device affected by latency. This parameter is sampled at 1 millisecond (ms)

intervals, and the counter is incremented if the condition is true. Each sample represents 1 ms of time with a 0 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 0.

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. This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

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	--

2 show fabric route pathinfo

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

2 show fabric route pathinfo

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-rbridgeld** *src-id*] [**dst-rbridgeld** *dst_id*]

Operands

src-rbridgeld	Specifies the source RBridge ID
<i>src-id</i>	Specifies details on the source RBridge.
dst-rbridgeld	Specifies the destination RBridge ID
<i>dst_id</i>	Specifies details on the destination RBridge.

Defaults None

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 source switch. Valid values range from 1 through 239.
Dst RB-ID	Destination rbridge-id to where the traffic flows. Valid values range 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	Neighbor Index of the ISL connected from local port.
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 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 parameter. 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.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1. This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

Examples To display the fabric route topology information:

```
switch# show fabric route topology
```

```
Total Path Count: 3
```

Src RB-ID	Dst RB-ID	Out Index	Out Interface	Hops	Cost	Nbr Index	Nbr 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

This example displays route topology details and includes the breakout index of the neighbor interface in normal mode.

```
sw0# show fabric route topology
```

```
Total Path Count: 3
```

Src RB-ID	Dst RB-ID	Out Index	Out Interface	Hops	Cost	Nbr Index	Nbr Interface	BW	Trunk
1	48	30	Te 1/0/49:1	1	500	1	Te 48/0/49:1	40G	Yes

This example displays route topology details and includes the breakout index of the neighbor interface in mixed mode running Network O.S. v4.0.0.

```
sw0# show fabric route topology
```

```
Total Path Count: 3
```

Src RB-ID	Dst RB-ID	Out Index	Out Interface	Hops	Cost	Nbr Index	Nbr Interface	BW	Trunk

2 show fabric route topology

```
1      48      30   Te 1/0/49      1      500      1      Te 48/0/49      40G      Yes
```

This example displays route topology details and includes the breakout index of the neighbor interface in mixed mode running Network O.S. v4.1.0.

```
sw0# show fabric route topology
```

Total Path Count: 3

Src RB-ID	Dst RB-ID	Out Index	Out Interface	Hops	Cost	Nbr Index	Nbr Interface	BW	Trunk
1	48	30	Te 1/0/49:1	1	500	1	Te 48/0/49	40G	Yes

See Also fabric route mcast

show fabric trunk

Displays Inter-Switch Link (ISL) trunk information.

Synopsis **show fabric trunk** [*rbridge-id* | **all**]

Operands *rbridge-id* Specifies the RBridge ID. 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 trunking information of ISL ports. The command displays the following fields:

Rbridge-id	RBridge ID of the switch. Valid values range 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 neighbor 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.

When a fabric is running normal mode (switches are running Network OS 4.1.0 or later), CLI output displays the QSFP breakout index for all switches in the fabric.

When a fabric is running mixed mode (switches are running Network OS 4.1.0 or earlier), the QSFP breakout index is not displayed in the output on switches running Network OS versions earlier than v4.1.0. In such instances, the neighbor port WWN (Nbr-WWN) is displayed as XX:XX:XX:XX:XX:XX:XX:XX.

This command displays ISL details, including the breakout index of the interface if breakout mode is configured on the source or neighbor interface.

2 show fabric trunk

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 Group	Src Index	Source Interface	Nbr Index	Nbr 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

This example displays trunk details and includes the breakout index of the neighbor interface in normal mode.

```
sw0# show fabric trunk
```

```
Rbridge-id: 1
```

Trunk Group	Src Index	Source Interface	Nbr Index	Nbr Interface	Nbr-WWN
1	74	Te 1/0/49:1	0	Te 48/0/49:1	XX:XX:XX:XX:XX:XX:XX:XX
1	76	Te 1/0/49:2	1	Te 48/0/49:2	XX:XX:XX:XX:XX:XX:XX:XX
1	80	Te 1/0/49:3	3	Te 48/0/49:3	XX:XX:XX:XX:XX:XX:XX:XX
1	78	Te 1/0/49:4	2	Te 48/0/49:4	XX:XX:XX:XX:XX:XX:XX:XX

Where XX:XX:XX:XX:XX:XX:XX:XX is the neighbor port WWN

This example displays trunk details and includes the breakout index of the neighbor interface in mixed mode running Network OS v4.0.0.

```
sw0# show fabric trunk
```

```
Rbridge-id: 1
```

Trunk Group	Src Index	Source Interface	Nbr Index	Nbr Interface	Nbr-WWN
1	74	Te 1/0/49	0	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX
1	76	Te 1/0/49	1	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX
1	80	Te 1/0/49	3	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX
1	78	Te 1/0/49	2	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX

This example displays trunk details and includes the breakout index of the neighbor interface in mixed mode running Network OS v4.1.0.

```
sw0# show fabric trunk
```

```
Rbridge-id: 1
```


Trunk Group	Src Index	Source Interface	Nbr Index	Nbr Interface	Nbr-WWN
1	74	Te 1/0/49:1	0	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX
1	76	Te 1/0/49:2	1	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX
1	80	Te 1/0/49:3	3	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX
1	78	Te 1/0/49:4	2	Te 48/0/49	XX:XX:XX:XX:XX:XX:XX:XX

See Also fabric trunk enable, show fabric isl, show fabric islports

show fcoe fabric-map

Displays the FCoE fabric-map configuration globally in a fabric, or on a single RBridge.

Synopsis **show fcoe fabric-map** [*rbridge-id rbridge-id*]

Operands **rbridge-id rbridge-id** Optionally selects the fabric-map configuration on a single RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the FCoE fabric-map on all or one of the RBridges in a fabric.

Usage Guidelines None

Examples To display the fabric-map configuration on all RBridges in the fabric:

```
switch# show fcoe-fabric-map
=====
Fabric-Map      VLAN      VFID      Pri    FCMAP      FKA      Timeout      Total-FCoE-Enodes
=====
default         1002[D]  128[D]   3[D]   0xefc00[D] 8000[D]  Enabled[D]   264
```

To display the fabric-map configuration for a single RBridge:

```
switch# show fcoe-fabric-map rbridge-id 19
=====
Fabric-Map      VLAN      VFID      Pri    FCMAP      FKA      Timeout      FCoE-Enodes
=====
default         1002[D]  128[D]   3[D]   0xefc00[D] 8000[D]  Enabled[D]   200
```

To display the fabric-map configuration where the number of FCoE ENodes is the default value:

```
switch# show fcoe-fabric-map rbridge-id 20
=====
Fabric-Map      VLAN      VFID      Pri    FCMAP      FKA      Timeout      FCoE-Enodes
=====
default         1002[D]  128[D]   3[D]   0xefc00[D] 8000[D]  Enabled[D]   64 [D]
```

To display the fabric-map configuration where no FCoE license is present:

```
switch# show fcoe-fabric-map rbridge-id 21
=====
Fabric-Map      VLAN      VFID      Pri    FCMAP      FKA      Timeout      FCoE-Enodes
=====
default         1002[D]  128[D]   3[D]   0xefc00[D] 8000[D]  Enabled[D]   0
```

The command **show running-config rbridge-id rbridge-id** also shows the status of “fabric-map” and “fcoe-enode” under “fcoe,” as in the following example:

```
sw0# show running-config rbridge-id 19
rbridge-id 19
:
```

```
fcoe
fabric-map default
fcoe-enode 200
!
```

```
sw0# show running-config rbridge-id 20
rbridge-id 20
:
fcoe
fabric-map default
fcoe-enode 64
!
```

```
sw0# show running-config rbridge-id 21
rbridge-id 21
:
fcoe
fabric-map default
fcoe-enode 0
!
```

See Also **fcoe-enodes**

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 RBridge ID.	
Defaults	None		
Command Modes	Privileged EXEC mode		
Description	Use this command to display 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** *vf_id*] [**vlan** *vlan_id*]

Operands	interface	Displays 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 <i>rbridge-id</i>	Displays FCoE logins for a given RBridge ID.
	vfid <i>vf_id</i>	Displays logins for an FCoE virtual fabric. Valid values range from 1 through 4096.
	vlan <i>vlan_id</i>	Displays logins for an FCoE VLAN. Refer to the Usage Guidelines.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display FCoE login information.

Usage Guidelines This command is not available in standalone mode.

NOTE

The FCoE virtual fabric is not to be confused with the Virtual Fabrics feature that supports service or transport VFs.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also None

show fcoe map

Displays all FCoE maps, or a single map.

Synopsis	show fcoe map [default { rbridge-id <i>rbridge-id</i> } rbridge-id <i>rbridge-id</i>]	
Operands	default	The fabric map name. The only map name available is “default”.
	rbridge-id <i>rbridge-id</i>	Specifies an RBridge ID.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to display all available FCoE maps, or a single designated map. However, for Network OS v4.1.0, the only map name allowed is “default.”	
Usage Guidelines	This command is not available in standalone mode.	
Examples	switch# show fcoe map default	
	=====	
	Name	DCB-Map FABRIC-MAP(s)
	=====	
See Also	default	default default
	None	

show fcsp auth-secret dh-chap

Displays the switches (WWNs) for which a shared secret is configured.

Synopsis **show fcsp auth-secret dh-chap**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the switch world wide names (WWNs) for which a shared secret is configured.

Usage Guidelines This command is supported only on Brocade VDX 6730 switches.

Examples switch# **show fcsp auth-secret dh-chap**
 10:00:00:05:1e:7a:c3:00

See Also fcsp auth, fcsp auth-secret dhchap, show running-config fcsp auth

show fibrechannel login

Displays fibrechannel logins.

Synopsis **show fibrechannel login** [**rbridge-id** *rbridge-id* | **interface** *fcoe-id*]

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID of the fibrechannel logins to display.
interface *fcoe-id* Specifies the FCoE interface name in VN-Num/RBridge-ID/port format of the fibrechannel logins to display.

Defaults None

Command Modes Privileged Exec mode

Description Displays fibrechannel logins for a specified fibrechannel interface or a specified RBridge ID.

Usage Guidelines None

Examples To view all fibrechannel:

```
sw0# show fibrechannel login
=====
===
Interface   Index  PID      status      protocol  speed      PortWWN
=====
===
Fi 17/0/3   2      110146   up(In_Sync  ) up        4G Auto    2e:83:00:05:33:26:14:26
Fi 17/0/3   2      110145   up(In_Sync  ) up        4G Auto    2d:07:00:05:33:26:14:26
Fi 17/0/3   2      110144   up(In_Sync  ) up        4G Auto    2e:fc:00:05:33:26:14:26
Fi 17/0/3   2      110143   up(In_Sync  ) up        4G Auto    20:74:00:05:33:26:14:26
Fi 17/0/3   2      110142   up(In_Sync  ) up        4G Auto    26:0a:00:05:33:26:14:26
Fi 17/0/3   2      110141   up(In_Sync  ) up        4G Auto    28:2d:00:05:33:26:14:26
Fi 17/0/3   2      110140   up(In_Sync  ) up        4G Auto    10:00:00:05:33:26:14:26
Fi 17/0/4   3      110100   up(In_Sync  ) up        4G Auto    10:00:00:05:33:26:14:27

Total number of Login(s) = 8
```

To view fibrechannel logins for an RBridge:

```
sw0# show fibrechannel login rbridge-id 17
=====
===
Interface   Index  PID      status      protocol  speed      PortWWN
=====
===
Fi 17/0/3   2      110146   up(In_Sync  ) up        4G Auto    2e:83:00:05:33:26:14:26
Fi 17/0/3   2      110145   up(In_Sync  ) up        4G Auto    2d:07:00:05:33:26:14:26
Fi 17/0/3   2      110144   up(In_Sync  ) up        4G Auto    2e:fc:00:05:33:26:14:26
Fi 17/0/3   2      110143   up(In_Sync  ) up        4G Auto    20:74:00:05:33:26:14:26
Fi 17/0/3   2      110142   up(In_Sync  ) up        4G Auto    26:0a:00:05:33:26:14:26
Fi 17/0/3   2      110141   up(In_Sync  ) up        4G Auto    28:2d:00:05:33:26:14:26
Fi 17/0/3   2      110140   up(In_Sync  ) up        4G Auto    10:00:00:05:33:26:14:26
Fi 17/0/4   3      110100   up(In_Sync  ) up        4G Auto    10:00:00:05:33:26:14:27

Total number of Login(s) = 8
```


To view fibrechannel logins on an interface:

```
sw0# show fibrechannel login interface 17/0/3
=====
===
Interface      Index    PID      status      protocol  speed      PortWWN
=====
===
Fi 17/0/3      2        110146   up(In_Sync  )  up        4G Auto    2e:83:00:05:33:26:14:26
Fi 17/0/3      2        110145   up(In_Sync  )  up        4G Auto    2d:07:00:05:33:26:14:26
Fi 17/0/3      2        110144   up(In_Sync  )  up        4G Auto    2e:fc:00:05:33:26:14:26
Fi 17/0/3      2        110143   up(In_Sync  )  up        4G Auto    20:74:00:05:33:26:14:26
Fi 17/0/3      2        110142   up(In_Sync  )  up        4G Auto    26:0a:00:05:33:26:14:26
Fi 17/0/3      2        110141   up(In_Sync  )  up        4G Auto    28:2d:00:05:33:26:14:26
Fi 17/0/3      2        110140   up(In_Sync  )  up        4G Auto    10:00:00:05:33:26:14:26

Total number of Login(s) = 7
```

See Also None

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 firmware download history for the switches.

Synopsis **show firmwaredownloadhistory [rbridge-id {rbridge-id | all}]**

Operands **rbridge-id** Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id Specifies a unique identifier for a node.

all Specifies all identifiers for a node.

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 Use this command to display information for the local management module only.

Examples To display the firmware download history:

switch# **show firmwaredownloadhistory**

Firmware version history					
Sno	Date & Time		Switch Name	Slot	PID OS Version
1	Thu May	2 05:00:08 2013	sw0	0	1561 nos4.0.0
2	Wed May	1 07:44:43 2013	sw0	0	1551 nos3.0.1

See Also **firmware commit, firmware download, show version**

show firmwaredownloadstatus

Displays the firmware download activity log.

Synopsis **show firmwaredownloadstatus** [**brief**] [**summary**] [**rbridge-id** {*rbridge-id* | **all**}]

Operands **brief** Displays only the last entry of the firmware download event log.

summary Displays a high-level summary of the firmware download status.

rbridge-id Executes the command on the specified switch.

rbridge-id Specifies the RBridge ID 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** operand is supported in VCS mode only.

 The output varies depending on the hardware platform.

Examples To display the firmware download event log on a 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.
```

2 show firmwaredownloadstatus

To display a high-level summary of the firmware download status:

```
switch# show firmwaredownloadstatus summary rbridge-id 1-4  
Rid 1: INSTALLING  
Rid 2: INSTALLED (Ready for activation)  
Rid 3: COMMITTING  
Rid 4: COMMITED
```

See Also **firmware commit, firmware download, firmware restore, show version, firmware activate, firmware recover, firmware download logical-chassis**

show global-running-config

Displays the global running configuration.

Synopsis	show global-running-config
Operands	None
Defaults	None
Command Modes	Privileged EXEC mode
Description	Displays the currently running global configuration for a node.
Usage Guidelines	None
Examples	The following example shows partial output for this command:

```
switch# show global-running-config
logging raslog console INFO
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
no support autoupload enable
support 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 user snmpadmin1 groupname snmpadmin
snmp-server user snmpadmin2 groupname snmpadmin
snmp-server user snmpadmin3 groupname snmpadmin
snmp-server user snmpuser1
snmp-server user snmpuser2
snmp-server user snmpuser3
line vty
  exec-timeout 10
!
zoning enabled-configuration cfg-name ""
zoning enabled-configuration default-zone-access allaccess
zoning enabled-configuration cfg-action cfg-save
role name admin desc Administrator
role name user desc User
aaa authentication login local
aaa accounting exec default start-stop none
aaa accounting commands default start-stop none
service password-encryption
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
```

2 show global-running-config

```
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-priority priority 0
!
fcoe
fabric-map default
vlan 1002
priority 3
virtual-fabric 128
fcmap 0E:FC:00
max-enodes 64
advertisement interval 8000
keep-alive timeout
!
map default
fabric-map default
cee-map default
!
!
interface Vlan 1
shutdown
!
interface Vlan 123
shutdown
protocol lldp
advertise dcbx-fcoe-app-tlv
advertise dcbx-fcoe-logical-link-tlv
advertise dcbx-tlv
system-description Brocade-VDX-VCS 300
!
vlan dot1q tag native
port-profile default
vlan-profile
switchport
switchport mode trunk
switchport trunk allowed vlan all
switchport trunk native-vlan 1
!
class-map cee
class-map default
```

See Also **show rbridge-running config, show rbridge-local-running-config**

show ha

Displays the High Availability (HA) status of the management modules.

Synopsis `show ha [all-partitions] [rbridge-id {rbridge-id} all]`

Operands

all-partitions	Displays the HA status for all partitions.
rbridge-id	Executes the command on the specified switch.
<i>rbridge-id</i>	Specifies the RBridge ID for the switch.
all	Specifies all switches in the VCS fabric.

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 non-disruptive.
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.

2 show ha

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
```

To display HA status for all partitions:

```
switch# show ha all-partitions  
Local (M2): Active, Cold Recovered  
Remote (M1): Standby, Healthy  
HA enabled, Heartbeat Up, HA State synchronized  
L2/0: Active, Cold Recovered, Dual Partitions, Redundant, State in sync  
1: Standby, Dual Partitions, Redundant, State in sync
```

See Also [ha enable](#), [ha failover](#), [ha failover](#)

show history

Displays the history of commands executed on the switch.

Synopsis **show history** [*number*]

Operands *number* The number of commands to display. If you omit this value, all commands are displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the history of commands executed on the switch.

Usage Guidelines None

Examples Typical command output display.

```
switch# show history
21:10:20 -- show arp vrf test
21:35:57 -- show ip
21:38:03 -- show arp vrf name
21:38:14 -- show access-
21:39:07 -- show access-list-log
21:39:18 -- show capture
21:48:53 -- show b int po
21:48:57 -- show bp
21:53:12 -- show cli
21:53:46 -- show cli
21:54:37 -- show cli
22:05:36 -- show confd-state cli listen ssh ip port
```

See Also None

show interface

Displays the detailed interface configuration and capabilities of all interfaces or for a specific interface.

Synopsis **show interface** [**fibrechannel** *rbridge-id/slot/port* | **management** *rbridge-id/slot/port* | **fcoe** [*vn-number/rbridge-id/front-port-number* | **rbridge-id** *rbridge-id*] | **fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **loopback** *number* | **port-channel** *number* | **stats** *rbridge-id/slot/port* | **switchport** | **tengigabitethernet** *rbridge-id/slot/port* | **vlan** *vlan_id*]

Operands	fibrechannel	See show interface FibreChannel .
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	loopback <i>number</i>	Specifies a loopback interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	management	See show interface management .
	fcoe	Specifies FCoE interfaces.
	<i>vn-number</i>	Specifies the VN number for FCoE.
	<i>rbridge-id</i>	Specifies the routing bridge ID. This is not valid in standalone mode.
	<i>front-port-number</i>	Specifies the front port number.
	rbridge-id <i>rbridge-id</i>	Specifies the routing bridge ID.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	port-channel <i>number</i>	Specifies to display the port-channel number. Valid values range from 1 through 63.
	stats	See show interface stats .
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.

<i>port</i>	Specifies a valid port number.
switchport	Specifies to display information for Layer 2 interfaces.
tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
vlan <i>vlan_id</i>	Specifies a VLAN interface. Refer to the Usage Guidelines.

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.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

If **show interface loopback** is executed in logical chassis cluster mode, loopback interfaces are not shown.

Examples To display detailed information for the 10-gigabit Ethernet interface 1/0/1:

```
switch# show interface tengigabitethernet 1/0/1
Ten Gigabit Ethernet 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
```

2 show interface

```
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-gigabit Ethernet interface on a Brocade VDX 6710 switch:

```
switch# show interface gigabitethernet 1/0/2
Gigabit Ethernet 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      : Ten Gigabit Ethernet 1/0/8
Switchport mode     : access
Ingress filter      : enable
Acceptable frame types : all
Default Vlan        : 1
Active Vlans        : 1
Inactive Vlans      : -

Interface name      : Ten Gigabit Ethernet 1/0/19
Switchport mode     : hybrid
Ingress filter      : enable
Acceptable frame types : all
Default Vlan        : 1
Active Vlans        : 1
```

```
Inactive Vlans           : 100

Interface name           : Ten Gigabit Ethernet 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 interface fibrechannel, show interface management, show ip interface**

show interface description

Displays the interface description.

Synopsis show interface description [**rbridge-id** *rbridge-id* | *range* | **all**]

Operands **rbridge-id** *rbridge-id* The unique identifier for a switch, or set of switches. The range of valid values is from 1 through 239.

range A range of *rbridge-id* values. The range string can be discontiguous, such as “1-3,5”.

all Selects all of the members of the logical chassis cluster.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display an interface description.

Usage Guidelines None

Examples Typical command output:

```
switch# show interface description
-----
Port                Type    Speed  Description
-----
Te 1/0/1            eth     10G    appcl12-c9c06-a05-swid1105-m1-sw
Te 1/0/2            eth     10G    --
Te 1/0/3            eth     10G    --
-----
Interface           Description
-----
Po 11                TO:appcl12-c9c06-a06-swid1106-sw-slot104
Po 12                TO:appcl12-c9c06-a06-swid1106-sw-slot105
```

See Also None

show interface FibreChannel

Displays Fibre Channel port hardware statistics.

Synopsis **show interface FibreChannel** *rbridge-id/slot/port* [**detail**]

Operands

<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
detail	Displays detailed error and statistics counters.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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.

after this, 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** parameter, 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 0 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, it shows "N/A".
Remaining Buffers	The remaining (unallocated and reserved) buffers in a port group.

NOTE

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 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: 0         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

```

2 show interface FibreChannel

```
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 information related to a management interface.

Synopsis **show interface management** [*rbridge-id/port*] [**ip** [**address** | **gateway-address**] | **ipv6** [**ipv6-address** | **ipv6-gateways**] [**line-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 standalone platforms, the port number for the management port is always 0.
On a modular switches with two redundant management modules, you can configure two management ports: 1 and 2.**ip**Displays the IPv4 configurations for the selected interface.

address Displays assigned IPv4 addresses.

gateway-address Displays assigned IPv4 gateway addresses.

ipv6 Displays the IPv6 configurations for the selected interface.

ipv6-address Displays assigned IPv6 addresses.

ipv6-gateways Displays assigned IPv6 gateway addresses.

line-speed Displays Ethernet speed and other line configurations for the selected interface.

Defaults This command is executed on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display information related to a management interface.

Usage Guidelines The address field indicates if DHCP is used to obtain an IP address or if a static IP address is used.

Examples The following example displays information related to a 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"
```

The following example displays information related to a 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"
```

2 show interface management

line-speed configured Auto

The following example displays information related to a management interface 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 interface stats

Displays interface statistics for a variety of interfaces.

Synopsis **show interface stats** {**brief** [*slot linecard_number*] | **detail** [**interface** [*fortygigabitethernet rbridge-id/slot/port* | *gigabitethernet rbridge-id/slot/port* | **port-channel** *number* | **tengigabitethernet rbridge-id/slot/port**] | **slot** *number*]}

Operands

brief	Displays summary statistics.
slot <i>linecard_number</i>	Displays statistics for specified linecard.
detail	Displays detailed statistics.
interface	Displays statistics for all interfaces or specific types of interface.
fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
port-channel <i>number</i>	Specifies a port-channel number. Valid values range from 1 through 6144.
tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
slot <i>number</i>	Specifies a slot.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view statistics for a variety of interface types.

Usage Guidelines None

Examples To display detailed statistics on a 10-GbE interface:

```
sw0# show interface stats detail interface ten 0/24
Interface TenGigabitEthernet 0/24 statistics (ifindex 403439639)
          RX
Packets      0      TX
Bytes        0
Unicasts     0
```

2 show interface stats

Multicasts	0	0
Broadcasts	0	0
Errors	0	0
Discards	0	0
Overruns	0	Underruns 0
Runts	0	
Jabbers	0	
CRC	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	0	
Mbits/Sec	0.000000	0.000000
Packet/Sec	0	0
Line-rate	0.00%	0.00%

See Also **show interface, show ip interface**

show interface status

Displays the interface status.

Synopsis **show interface status** [**rbridge-id** *rbridge-id* | *range* | **all**]

Operands **rbridge-id** *rbridge-id* The unique identifier for a switch, or set of switches. The range of valid values is from 1 through 239.

range A range of *rbridge-id* values. The range string can be discontinuous, such as "1-3,5".

all Selects all of the members of the logical chassis cluster.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display interface status.

Usage Guidelines None

Examples Typical command output:

```
switch# show interface status
```

Port	Status	Vlan	Speed	Type	Description
Te 1/0/1	connected	Trunk	10G	10G-SFPP-LR	
Te 1/0/2	connected	1	10G	10G-SFPP-SR	
Po 1	connected	Trunk	40G	--	
Po 2	connected	1	20G	--	

See Also None

show interface trunk

Displays the interface trunk information.

Synopsis	show interface trunk [rbridge-id <i>rbridge-id</i> <i>range</i> all]	
Operands	rbridge-id <i>rbridge-id</i>	The unique identifier for a switch, or set of switches. The range of valid values is from 1 through 239.
	<i>range</i>	A range of <i>rbridge-id</i> values. The range string can be discontinuous, such as “1-3,5”.
	all	All of the members of the logical cluster.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to display interface trunk information.	
Usage Guidelines	None	
Examples	Typical command output:	
	<pre>switch# show interface trunk ----- Port Vlans Allowed on Trunk ----- Te 1/0/1 1-4094 Te 1/0/2 1-4094 Te 1/0/3 1-4094 Po 52 1-4094 Po 99 1-4094 Po 401 701-703,757,2200-2399 Po 403 701-703,757,2200-2399 Po 405 701-703,757,2200-2399 Po 407 701-703,757,2200-2399</pre>	
See Also	None	

show inventory

Displays the hardware inventory of the switch.

Synopsis **show inventory** [**chassis** | **fan** | **module** | **powerSupply**]

Operands	chassis	Displays information about the chassis.
	fan	Displays information about the fan.
	module	Displays information about the module.
	powerSupply	Displays information about the power supply.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the hardware inventory of the switch.

Usage Guidelines None

Examples Example of typical command output

```
switch# show inventory
NAME:MM, Slot M1      DESCR:Chassis Blade module
PN:60-1002179-23      SN:BVT0417J00M

NAME:MM, Slot M2      DESCR:Chassis Blade module
PN:60-1002179-13      SN:BVT0302H00T

NAME:SFM, Slot S1     DESCR:Chassis Blade module
PN:60-1002180-12      SN:BVU0304H037

NAME:SFM, Slot S2     DESCR:Chassis Blade module
PN:60-1002180-12      SN:BVU0302H01Y

NAME:SFM, Slot S3     DESCR:Chassis Blade module
PN:60-1002560-01      SN:BVU0307H01G

NAME:LC, Slot L1      DESCR:Chassis Blade module
PN:60-1002466-17      SN:CCE0423J00P

NAME:LC, Slot L2      DESCR:Chassis Blade module
PN:60-1002466-09      SN:CCE0315H00B

NAME:LC, Slot L3      DESCR:Chassis Blade module
PN:60-1002569-01      SN:CCE0305H00G

NAME:LC, Slot L4      DESCR:Chassis Blade module
PN:60-1002181-12      SN:BVV0303H019

NAME:POWER SUPPLY 1   DESCR:Chassis PS module
PN:23-0000135-02      SN:BMM2J25G998

NAME:POWER SUPPLY 2   DESCR:Chassis PS module
PN:23-0000135-02      SN:BMM2J25G803
NAME: Chassis         DESCR:System Chassis
```

2 show inventory

```
SID:BR-VDX8770-4      SwitchType:1000
PN:84-1001681-03     SN:BZA0305H00D
```

See Also None

show ip bgp

Displays BGP information.

Synopsis **show ip bgp** {**summary**} [**rbridge-id** *rbridge-id*]

Operands	summary	Displays the local autonomous system number (ASN), maximum number of routes supported, and some BGP4 statistics.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view BGP information.

Usage Guidelines None

Examples switch# **show ip bgp**

See Also None

show ip bgp attribute-entries

Displays BGP4 route-attribute entries that are stored in device memory.

Synopsis **show ip bgp attribute-entries** [**rbridge-id** *rbridge-id*]

Operands **rbridge-id** Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description The route-attribute entries table lists the sets of BGP4 attributes that are stored in device memory. Each set of attributes is unique and can be associated with one or more routes. In fact, the device typically has fewer attribute entries than routes. Use this command to view BGP4 route-attribute entries that are stored in device memory.

Usage Guidelines None

Examples switch# **show ip bgp attribute-entries**

See Also None

show ip bgp dampened-paths

Displays all BGP4 dampened routes.

Synopsis **show ip bgp dampened-paths** [**rbridge-id** *rbridge-id*]

Operands **rbridge-id** Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id None
Specifies a
unique identifier
for a
node.**Defaults**

Command Modes Privileged EXEC mode

Description Use this command to view all BGP4 dampened routes.

Usage Guidelines None

Examples switch# **show ip bgp dampened-paths**

See Also None

show ip bgp filtered-routes

Displays BGP4 filtered routes that are received from a neighbor or peer group.

Synopsis	show ip bgp filtered-routes { detail } [<i>ip-addr</i> [/ <i>mask</i>] [longer-prefixes]] as-path-access-list <i>name</i>] prefix-list <i>name</i>] [rbridge-id <i>rbridge-id</i>]	
Operands	detail	Optionally displays detailed route information.
	<i>ip-addr</i>	IPv4 address of the destination network in dotted-decimal notation.
	<i>mask</i>	(Optional) IPv4 mask of the destination network in CIDR notation.
	longer-prefixes	Specifies all statistics for routes that match the specified route, or that have a longer prefix than the specified route.
	as-path-access-list	Specifies an AS-path ACL.
	prefix-list	Specifies an IP prefix list.
	<i>name</i>	Name of an AS-path ACL or prefix list.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to view BGP4 filtered routes that are received from a neighbor or peer group.	
Usage Guidelines	None	
Examples	switch# show ip bgp filtered-routes detail 10.11.12.13 prefix-list	
See Also	None	

show ip bgp flap-statistics

Displays BGP4 route-dampening statistics for all dampened routes with a variety of options.

Synopsis **show ip bgp flap-statistics** [*ip-addr* [/*mask*]] [**longer-prefixes**]] | **as-path-filter** *name*] | **neighbor** *ip-addr*] | [**regular-expression** *name*] [**rbridge-id** *rbridge-id*]

Operands	detail	Optionally displays detailed route information.
	<i>ip-addr</i>	IPv4 address of a specified route in dotted-decimal notation.
	<i>mask</i>	(Optional) IPv4 mask of a specified route in CIDR notation.
	as-path-filter name	Specifies an AS-path filter.
	longer-prefixes	Displays statistics for routes that match the specified route or have a longer prefix than the specified route.
	neighbor	Displays flap statistics only for routes learned from the specified neighbor.
	<i>ip-addr</i>	IPv4 address of the neighbor.
	regular-expression	Specifies a regular expression in the display output on which to filter.
	<i>name</i>	Name of an AS-path filter or regular expression.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view BGP4 route-dampening statistics for all dampened routes with selected options.

Usage Guidelines None

Examples switch# **show ip bgp flap-statistics neighbor 10.11.12.13**

See Also None

show ip bgp neighbor

Displays configuration information and statistics for BGP4 neighbors of the device.

Synopsis **show ip bgp neighbor** *ip-addr* [**rbridge-id** *rbridge-id*]

Operands	<i>ip-addr</i>	IPv4 address of the neighbor in dotted-decimal notation.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view configuration information and statistics for BGP4 neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

Usage Guidelines None

Examples switch# **show ip bgp neighbor 10.11.12.13**

See Also None

show ip bgp neighbors

Displays configuration information and statistics for BGP4 neighbors of the device.

Synopsis **show ip bgp neighbors** {*ip-addr* | **route-summary** | **last-packet-with-error**} [**rbridge-id** *rbridge-id*]

Operands	<i>ip-addr</i>	IPv4 address of a neighbor in dotted-decimal notation.
	route-summary	Displays routes received, routes accepted, number of routes advertised by peer, and so on.
	last-packet-with-error	Displays the last packet with an error.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view configuration information and statistics for BGP4 neighbors of the device. Output shows all configured parameters for the neighbors. Only the parameters whose values differ from defaults are shown.

Usage Guidelines None

Examples switch# **show ip bgp neighbors route-summary**

See Also None

show ip bgp neighbors advertised-routes

Displays configuration information and statistics for BGP4 neighbors of the device.

Synopsis	show ip bgp neighbors <i>ip-addr</i> advertised-routes { detail <i>ip-addr</i> {/mask-bits}} [rbridge-id <i>rbridge-id</i>]	
Operands	<i>ip-addr</i>	IPv4 address of a neighbor in dotted-decimal notation.
	advertised-routes	Displays only the routes that the device has advertised to the neighbor during the current BGP4 session.
	detail	Displays details of advertised routes.
	<i>mask-bits</i>	Number of mask bits in CIDR notation.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to view configuration information and statistics for BGP4 neighbors of the device.	
Usage Guidelines	None	
Examples	switch# show ip bgp neighbors 10.11.12.13 advertised-routes detail	
See Also	None	

show ip bgp neighbors flap-statistics

Displays configuration information and flap statistics for BGP4 neighbors of the device.

Synopsis **show ip bgp neighbors** *ip-addr* **flap-statistics** [**rbridge-id** *rbridge-id*]

Operands	<i>ip-addr</i>	IPv4 address of a neighbor in dotted-decimal notation.
	flap-statistics	Displays the route flap statistics for routes received from or sent to a neighbor.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view configuration information and flap statistics for BGP4 neighbors of the device.

Usage Guidelines None

Examples switch# **show ip bgp neighbors 10.11.12.13 flap-statistics**

See Also None

show ip bgp neighbors received

Displays Outbound Route Filters (ORFs) received from BGP4 neighbors of the device.

Synopsis **show ip bgp neighbors** *ip-addr* **received** [**extended-community** | **prefix-filter**] [**rbridge-id** *rbridge-id*]

Operands	<i>ip-addr</i>	IPv4 address of a neighbor in dotted-decimal notation.
	extended-community	Displays the results for ORFs that use the BGP Extended Community Attribute.
	prefix-filter	Displays the results for ORFs that are prefix-based.
	rbridge-id	Enables RBridge ID mode to support VCS on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view ORFs received from BGP4 neighbors of the device.

Usage Guidelines None

Examples `switch# show ip bgp neighbors 10.11.12.13 received extended-community`

See Also None

show ip bgp neighbors received-routes

Lists all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

Synopsis **show ip bgp neighbors** *ip-addr* **received-routes** [**detail**] [**rbridge-id** *rbridge-id*]

Operands *ip-addr* IPv4 address of a neighbor in dotted-decimal notation.

detail Displays detailed route information.

rbridge-id Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view all route information received in route updates from BGP4 neighbors of the device since the soft-reconfiguration feature was enabled.

Usage Guidelines None

Examples switch# **show ip bgp neighbors 10.11.12.13 received-routes**

See Also None

show ip bgp neighbors routes

Lists a variety of route information received in UPDATE messages from BGP4 neighbors.

Synopsis **show ip bgp neighbors** *ip-addr* **routes** {**best** | **not-installed-best** | **unreachable**} | **detail** {**best** | **not-installed-best** | **unreachable**} [**rbridge-id** *rbridge-id*]

Operands	<i>ip-addr</i>	IPv4 address of a neighbor in dotted-decimal notation.
	best	Displays routes received from the neighbor that are the best BGP4 routes to their destination.
	not-installed-best	Displays routes received from the neighbor that are the best BGP4 routes to their destination but were not installed in the route table because the device received better routes from other sources.
	unreachable	Displays routes that are unreachable because the device does not have a valid RIP, OSPF, or static route to the next hop.
	detail	Displays detailed information for the specified route types.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view a variety of route information received in route updates from BGP4 neighbors of the device.

Usage Guidelines None

Examples To view best-route information received in UPDATE messages:

switch# **show ip bgp neighbors 10.11.12.13 routes best**

See Also None

show ip bgp neighbors routes-summary

Lists all route information received in UPDATE messages from BGP4 neighbors.

Synopsis **show ip bgp neighbors** *ip-addr* **routes-summary** [**rbridge-id** *rbridge-id*]

Operands	<i>ip-addr</i>	IPv4 address of a neighbor in dotted-decimal notation.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view all route information received in route updates from BGP4 neighbors of the device.

Usage Guidelines None

Examples switch# **show ip bgp neighbors 10.11.12.13 routes-summary**

See Also None

2 show ip bgp peer-group

show ip bgp peer-group

Displays peer-group information.

Synopsis **show ip bgp peer-group** *peer-group-name* [**rbridge-id** *rbridge-id*]

Operands	<i>ip-addr</i>	IPv4 address of a neighbor in dotted-decimal notation.
	<i>peer-group-name</i>	Peer-group name configured by the neighbor <i>peer-group-name</i> command.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view peer-group information. Only the parameters that differ from defaults are listed.

Usage Guidelines None

Examples switch# **show ip bgp peer-group mypeergroup**

See Also **neighbor**

show ip bgp routes

Displays BGP4 route information that is filtered by the table entry at which the display starts.

Synopsis **show ip bgp routes** *num* [**rbridge-id** *rbridge-id*]

Operands	<i>num</i>	Table entry at which the display starts.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view BGP4 route information that begins with a table entry defined by *num*.

Usage Guidelines None

Examples switch# **show ip bgp routes 100**

See Also None

show ip bgp routes age

Displays BGP4 route information that is filtered by age, best/not best routes, or routes not installed.

Synopsis **show ip bgp routes** [**age** *num* | **best** | **no-best** | **cidr-only** | **not-installed-best**] [**rbridge-id** *rbridge-id*]

Operands	age	Displays only those routes that have been received or updated more recently than the number of seconds specified by <i>num</i> .
	<i>num</i>	Last update interval, in seconds.
	best	Displays only routes received from a neighbor that the device selected as best routes.
	no-best	Displays only routes received from a neighbor that the device selected as suboptimal routes.
	cidr-only	Displays only routes whose network masks do not match their class network length.
	not-installed-best	Displays only routes received from a neighbor that are the best BGP4 routes to their destinations, but that were not installed in the IP route table because the device received better routes from other sources (such as OSPF, RIP, or static routes).
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view BGP4 route information that is controlled by the operands.

Usage Guidelines None

Examples To view BGP4 best route information:

```
switch# show ip bgp routes best
```

See Also None

show ip bgp routes as-path-access-list

Displays BGP4 route information that is filtered by autonomous system (AS)-path access control list (ACL).

Synopsis **show ip bgp routes** [**as-path-access-list** *name*] [**rbridge-id** *rbridge-id*]

Operands	as-path-access-list	Displays only those routes that use the AS-path ACL defined by <i>name</i> .
	<i>name</i>	Name of AS-path ACL.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view BGP4 route information that is filtered by AS-path ACL.

Usage Guidelines None

Examples To view BGP4 routes filtered by AS-path ACL:

```
switch# show ip bgp routes as-path-access-list myacl
```

See Also None

show ip bgp routes community

Displays BGP4 route information that is filtered by community and other options.

Synopsis	show ip bgp routes [community <i>num</i> internet local-as no-advertise no-export] [rbridge-id <i>rbridge-id</i>]	
Operands	community	Displays routes filtered by a variety of communities.
	<i>num</i>	Specific community member.
	internet	Displays routes for the Internet community.
	local-as	Displays routes for a local sub-AS within the confederation.
	no-advertise	Displays routes with this community that cannot be advertised to any other BGP4 devices at all.
	no-export	Displays routes for the community of sub-ASs within a confederation.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to view BGP4 route information that is filtered by community and other options.	
Usage Guidelines	None	
Examples	To view BGP4 routes filtered by community:	
	switch# show ip bgp routes community 10	
See Also	None	

show ip bgp routes community-access-list

Displays BGP4 route information for an AS-path community access list.

Synopsis **show ip bgp routes community-access-list** *name* [**rbridge-id** *rbridge-id*]

Operands	<i>name</i>	Name of the AS path community access list. Range is from 1 through 32 ASCII characters.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view BGP4 route information for an AS-path community access list.

Usage Guidelines None

Examples To view BGP4 route information for an AS-path community access list:

```
switch# show ip bgp routes community-access-list mycommunityacl
```

See Also None

show ip bgp routes community-reg-expression

Displays BGP4 route information for an ordered community-list regular expression.

Synopsis **show ip bgp routes community-reg-expression** *expression* [**rbridge-id** *rbridge-id*]

Operands	<i>expression</i>	An ordered community-list regular expression.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view BGP4 route information for an ordered community-list regular expression.

Usage Guidelines None

Examples To view BGP4 route information for an ordered community-list regular expression:

switch# **show ip bgp routes community-reg-expression myregexpression**

See Also None

show ip bgp routes longer-prefixes

Displays BGP4 route information that is filtered for a specific prefix and mask, as well as for prefixes with a longer mask than the one specified.

Synopsis **show ip bgp routes** *ip-addr/prefix* [**longer-prefixes** | *ip-addr*] [**rbridge-id** *rbridge-id*]

Operands	<i>ip-addr</i>	IPv4 address in dotted-decimal notation.
	<i>prefix</i>	Mask length in CIDR notation.
	longer-prefixes	Filters on prefixes equal to or greater than that specified by the mask.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view BGP4 route information for a specific prefix with a mask longer than or equal to the mask specified in the command.

Usage Guidelines None

Examples To view BGP4 route information filtered by longer prefixes:

```
switch# show ip bgp routes 10.11.12.12/23 longer-prefixes
```

See Also None

show ip bgp routes neighbor nexthop local unreachable

Displays BGP4 route information that is filtered by neighbor, next hop, and other options.

Synopsis	show ip bgp routes [neighbor <i>ip-addr</i> nexthop <i>ip-addr</i> local unreachable] [rbridge-id <i>rbridge-id</i>]	
Operands	neighbor	Displays only those routes that are received from the specified neighbor.
	nexthop	Displays only those routes that are received from the specified next hop.
	<i>ip-addr</i>	IPv4 address of neighbor or next hop, in dotted-decimal notation.
	local	Displays only those routes that use a Local AS.
	unreachable	Displays only those routes whose destinations are unreachable through any of the BGP4 paths in the BGP4 route table.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to view BGP4 route information that is filtered by neighbor, next hop, and other options.	
Usage Guidelines	None	
Examples	To view BGP4 routes filtered by neighbor:	
	switch# show ip bgp routes neighbor 10.11.12.13	
See Also	None	

show ip bgp routes summary detail

Displays BGP4 summary route information.

Synopsis **show ip bgp routes** [**summary** | **detail**] [**rbridge-id** *rbridge-id*]

Operands	summary	Displays summary route information.
	detail	Displays detailed route information.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view BGP4 summary or detailed information.

Usage Guidelines None

Examples To view summary BGP4 route information:

switch# **show ip bgp routes summary**

See Also None

show ip dhcp relay address interface

Displays IP DHCP Relay addresses configured on a specific interface.

Synopsis `show ip dhcp relay address interface [gigabitethernet rbridge-id/slot/port | tengigabitethernet rbridge-id/slot/port | fortygigabitethernet rbridge-id/slot/port]`

`show ip dhcp relay address interface ve vlan_id {rbridge-id rbridge-id | all | range}`

Operands

gigabitethernet *rbridge-id/slot/port* A valid 1-gigabit Ethernet interface.

- rbridge-id* Specifies the RBridge ID. This is not valid in standalone mode.
- slot* Specifies a valid slot number.
- port* Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port* A valid 10-gigabit Ethernet interface.

- rbridge-id* Specifies the RBridge ID. This is not valid in standalone mode.
- slot* Specifies a valid slot number.
- port* Specifies a valid port number.

fortygigabitethernet *rbridge-id/slot/port* A valid 40-gigabit Ethernet interface.

- rbridge-id* Specifies the RBridge ID. This is not valid in standalone mode.
- slot* Specifies a valid slot number.
- port* Specifies a valid port number.

ve VE interface.

vlan_id VLAN identification for interface.

rbridge-id *rbridge-id* Specific RBridge identification. You can specify multiple RBridge IDs, separated by commas.

all All RBridge IDs in the logical chassis cluster.

range A range of RBridge IDs separated by a dashes or commas, for example:

- 1-3 - RBridge ID 1 through 3
- 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5
- 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Defaults If the **rbridge-id** keyword is omitted, IP DHCP Relay addresses display for the local switch.

Command Modes Privileged EXEC mode

Description Display IP DHCP Relay addresses configured on specific physical or virtual Ethernet (VE) interfaces located on a local switch, specific switches, or all switches in a logical chassis cluster.

Usage Guidelines No spaces are allowed in the range string. The range does not need to be contiguous (for example, 1-2,5).

The **gigabitethernet *rbridge-id/slot/port*** parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches. The prompt for configuring these ports is in the following format:

```
switch(config-if-te-22/0/1)#
```

2 show ip dhcp relay address interface

Examples Display configured IP DHCP Relay addresses on a specific physical interface:

```
sw0# show ip dhcp relay address interface tengigabitethernet 1/0/24
```

```

                                     Rbridge Id: 1
                                     -----
Interface                           Relay Address      VRF Name
-----                           -
Te 1/0/24                           10.3.4.5         default-vrf
Te 1/0/24                           10.5.1.1         blue
```

Display configured IP DHCP Relay addresses on VE interface for RBridge ID 1.

```
sw0# show ip dhcp relay addresss int ve 300 rbridge-id 1
```

```

                                     Rbridge Id: 1
                                     -----
Interface                           Relay Address      VRF Name
-----                           -
Ve 300                             10.0.1.2         default-vrf
```

Display configured IP DHCP Relay addresses on VE interface on RBridge IDs 1 and 3.

```
sw0# show ip dhcp relay address interface ve 300 rbridge-id 1,3
```

```

                                     Rbridge Id: 1
                                     -----
Interface                           Relay Address      VRF Name
-----                           -
Ve 300                             10.0.1.2         default-vrf

                                     Rbridge Id: 3
                                     -----
Ve 300                             10.0.0.5         default-vrf
```

See Also ip dhcp relay address, show ip dhcp relay address rbridge-id

show ip dhcp relay address rbridge-id

Displays IP DHCP Relay addresses.

Synopsis `show ip dhcp relay address rbridge-id rbridge-id | all | range`

Operands

<i>rbridge-id</i>	Specific RBridge identification. You can specify multiple RBridge IDs, separated by commas.
all	All RBridge IDs in the logical chassis cluster.
<i>range</i>	A range of RBridge IDs separated by a dashes or commas, for example: 1-3 - RBridge ID 1 through 3 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Defaults If the *rbridge-id* parameter is omitted, IP DHCP Relay addresses display for the local switch.

Command Modes Privileged EXEC mode

Description Displays the IP address and Virtual Routing and Forwarding (VRF) name for all interfaces with configured IP DHCP Relay addresses on a local switch, specific switches, or all switches in a VCS Fabric cluster.

Usage Guidelines No spaces are allowed in the *range* string. The range does not need to be contiguous (for example, 1-2,5).

Examples To display addresses configured on a specific RBridge ID:

```
sw0# show ip dhcp relay address rbridge-id 2
```

```

                                     Rbridge Id:    2
                                     -----
Interface                          Relay Address      VRF Name
-----
Te 2/2/1                          10.1.1.1          Blue
Te 2/4/2                          20.1.1.1          Blue
Te 2/5/4                          30.1.1.1          Default-vrf
Te 2/6/6                          40.1.1.1          Green

```

To display addresses configured on all switches in a virtual fabric cluster:

```
sw0# show ip dhcp rel address rbridge-id all
```

```

                                     Rbridge Id:    1
                                     -----
Interface                          Relay Address      VRF Name
-----
Te 1/0/24                          2.3.4.5           default-vrf
Ve 300                             10.0.1.2           default-vrf

                                     Rbridge Id:    3
                                     -----
Interface                          Relay Address      VRF Name
-----
Ve 300                             10.0.0.5           default-vrf

```

2 `show ip dhcp relay address rbridge-id`

See Also `show ip dhcp relay address interface`, `ip dhcp relay address`

show ip dhcp relay statistics

Displays the general information about the DHCP Relay function.

Synopsis **show ip dhcp relay statistics** [**ip-address** *ip-addr*] [**rbridge-id** *rbridge-id* | **all** | *range*]

Operands **ip-address** *ip-addr* IPv4 address of DHCP server where client requests are to be forwarded.

rbridge-id *rbridge-id* Specific RBridge identification. You can specify multiple RBridge IDs, separated by commas.

all All RBridge IDs in the logical chassis cluster.

range A range of RBridge IDs separated by a dashes or commas, for example:

 1-3 - RBridge ID 1 through 3

 1-3, 5 - RBridge ID 1 through 3 and RBridge ID 5

 1, 3, 5, 6 - RBridge ID 1, 3, 5, and 6

Defaults If the *rbridge-id* parameter is omitted, IP DHCP Relay statistics display for the local switch. If the **ip-address** parameter is omitted, statistics display for all configured addresses on defined switches.

Command Modes Privileged EXEC mode

Description The following information is displayed about the IP DHCP Relay function for IP DHCP Relay addresses configured on a local switch, specific switches, or all switches in a logical chassis cluster:

- DHCP Server IP Address configured in the switch.
- Number of DHCP DISCOVERY, OFFER, REQUEST, ACK, NAK, DECLINE, and RELEASE packets received.
- Number of DHCP client packets received (on port 67) and relayed by the Relay Agent.
- Number of DHCP server packets received (on port 67) and relayed by the Relay Agent.

Usage Guidelines No spaces are allowed in the *range* string. The range does not need to be contiguous (for example, 1-2,5). You can also specify **all** for all RBridge IDs in a logical chassis cluster. To display addresses for configured interfaces on a local switch, an RBridge ID parameter is not required.

Examples To display statistics for a local switch:

sw0# show ip dhcp relay statistics

DHCP Relay Statistics - Rbridge Id: 3								
Address	Disc.	Offer	Req.	Ack	Nak	Decline	Release	Inform
10.1.0.1	400	100	2972	2968	0	0		0
20.2.0.1	400	100	2979	2975	0	0	0	0
30.3.0.1	400	100	3003	2998	0	0	0	0
40.4.0.1	400	100	3026	3018	0	0	0	0
Active Clients: 400								
Clients to Restore: 0								
Client Packets: 12780								
Server Packets: 12359								
Timed Out: 0								

2 show ip dhcp relay statistics

No Offers: 0

To display statistics for specific RBridge IDs:

```
sw0# show ip dhcp relay statistics rbridge-id 1,3
```

```

DHCP Relay Statistics - Rbridge Id: 1
-----
Address      Disc. Offer  Req.  Ack  Nak  Decline  Release  Inform
-----
2.3.4.5      300    100    1211  2968  0      0        0        0
10.0.1.2     300    100    1207  2975  0      0        0        0
```

Client Packets: 2701

Server Packets: 2932

```

DHCP Relay Statistics - Rbridge Id: 3
-----
Address      Disc. Offer  Req.  Ack  Nak  Decline  Release  Inform
-----
10.0.0.5      0        0        0        0        0        0        0        0
10.0.1.2      0        0        0        0        0        0        0        0
```

Client Packets: 0

Server Packets: 0

See Also **show ip dhcp relay address interface, show ip dhcp relay address rbridge-id, show ip dhcp relay statistics,**

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]] rbridge-id { <i>rbridge-id</i> all } [interface [fortygigabitethernet <i>rbridge-id/slot/port</i> tengigabitethernet <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i> ve [<i>vlan_id</i> rbridge-id <i>rbridge-id</i>] [detail A.B.C.D]] [interface <i>vlan</i> <i>vlan_id</i> detail] [interface port-channel <i>number</i> 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.
	rbridge-id <i>rbridge-id</i>	Specifies an RBridge. This is not valid in standalone mode.
	all	Displays all information.
	interface	Use this parameter to specify the interface.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the routing bridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the routing bridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface
	<i>rbridge-id</i>	Specifies the routing bridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	ve <i>vlan_id</i>	Specifies the virtual Ethernet (VE) interface. Refer to the Usage Guidelines.
	detail	Displays the IGMPv3 source information.
	interface	Use this parameter to specify the interface.
	vlan <i>vlan_id</i>	Specifies which VLAN interface to display the snooping configuration related information. Refer to the Usage Guidelines.
	detail	Displays the IGMPv3 source information.
	interface	Use this parameter to specify the interface.

port-channel number

Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.

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 switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

In logical chassis mode, when **rbridge-id** is specified, groups learned on Layer 3 interfaces for that particular RBridge ID are displayed. However, groups learned on Layer 2 interfaces from all the nodes in an entire cluster are displayed.

In logical chassis mode, if **rbridge-id** is not specified, IGMP groups on Layer 3 interfaces of the node on which the command is executed are displayed. Groups learned on Layer 2 interfaces from all the nodes in the cluster are displayed.

In logical chassis mode, when **rbridge-id all** is specified, all groups from all the nodes in the cluster are displayed.

Examples

This is an example of a detailed output.

```
switch# show ip igmp groups interface tengigabitethernet 125/1/32 detail
Interface: Te 125/1/32
Group: 225.225.1.1
Uptime: 00:02:45
Expires: 00:03:56
Last reporter: 125.32.1.3
Last reporter mode: IGMP V2
```

This is an example of a virtual interface output.

```
switch# show ip igmp groups interface ve 2006

Total Number of Groups: 1
IGMP Connected Group Membership
Group Address  Interface  Uptime      Expires     Last Reporter
226.226.1.1    Vlan 2006  00:00:09    00:04:03   112.26.1.25
Member Ports: Te 125/2/12
```

See Also None

show ip igmp interface

Displays information related to VLANs in the IGMP protocol module.

Synopsis **show ip igmp interface** [vlan *vlan_id* [[A.B.C.D [detail]]] | **rbridge-id** {*rbridge-id* | **all**} | [**interface** [fortygigabitethernet *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **ve** [vlan_id | **rbridge-id** *rbridge-id*] [detail | A.B.C.D]] | [**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.

rbridge-id *rbridge-id* Specifies an RBridge. This is not valid in standalone mode.

all Displays all information.

interface Use this parameter to specify the interface.

vlan *vlan_id* Specifies a VLAN interface. Refer to the Usage Guidelines.

fortygigabitethernet *rbridge-id/slot/port* Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the routing bridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port* Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the routing bridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port* Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the routing bridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

ve *vlan_id* Specifies a Virtual Ethernet (VE) interface. Refer to the Usage Guidelines.

detail Displays the IGMPv3 source information.

interface Use this parameter to specify the interface.

detail Displays the IGMPv3 source information.

interface Use this parameter to specify the interface.

	port-channel <i>number</i> Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144. detail Displays the IGMPv3 source information.
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 switches, 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. In logical chassis mode: • When the rbridge-id option is specified, details for the VE interface on that particular rbridge are displayed. • If rbridge-id is not specified, details for the VE interface on the node on which the command is executed is displayed. • When rbridge-id all is specified, all VE interfaces with that rbridge-id from all the nodes in the cluster are displayed.
Examples	<pre>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</pre>
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 the Usage Guidelines.

```
mrrouter interface vlan vlan_id
```

Specifies which VLAN interface to display the snooping configuration related information. Refer to the Usage Guidelines.

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 switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples To display IGMP snooping information for VLAN 5:

```
switch# show ip igmp snooping interface vlan 5
```

See Also None

show ip igmp statistics

Displays IGMP statistics.

Synopsis **show ip igmp statistics interface** [**interface** **fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **vlan** *vlan_id* | **ve** *vlan_id* [*rbridge-id rbridge-id*]]

Operands **fortygigabitethernet** *rbridge-id/slot/port*
 Specifies a valid 40gigabit Ethernet interface.

rbridge-id Specifies the routing bridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the routing bridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface

rbridge-id Specifies the routing bridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number. **vlan** *vlan_id* Specifies which VLAN interface to display the snooping configuration related information. Refer to the Usage Guidelines.

ve *vlan_id* Specifies a virtual Ethernet (VE) interface. Refer to the Usage Guidelines.

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

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display IGMP statistics for 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

In logical chassis mode:

2 show ip igmp statistics

- When the **rbridge-id** option is specified, details for the VE interface on that particular rbridge are displayed.
- If **rbridge-id** is not specified, details for the VE interface on the node on which the command is executed is displayed.
- When **rbridge-id all** is specified, all VE interfaces with that **rbridge-id** from all the nodes in the cluster are displayed.

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** {**rbridge-id** *rbridge-id* | **all**} | **fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **loopback** *number* | **port-channel** *number* | **tengigabitethernet** *rbridge-id/slot/port* | **ve** *vlan_id*]

Operands

brief Specifies to display a brief summary of IP interface status and configuration.

rbridge-id Specifies to display IP interface entries for a specific RBridge ID.

all Specifies to display IP interface entries for all RBridge IDs in the VCS cluster.

fortygigabitethernet *rbridge-id/slot/port* Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port* Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

loopback *number* Specifies to display the loopback interface number. Valid values range from 1 through 255.

port-channel *number* Specifies to display the port-channel number. Valid values range from 1 through 6144.

tengigabitethernet *rbridge-id/slot/port* Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

ve *vlan_id* Specifies a virtual Ethernet (VE) interface (VLAN interface number). Refer to the Usage Guidelines.

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* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Note the following with respect to the **show ip interface brief** command:

- The command **show ip interface brief rbridge-id rbridge-id** provides information about all physical, loopback, and switched virtual interfaces (SVIs) specific to the given *rbridge-id*.
- The command **show ip interface brief rbridge-id all** provides information about all physical, loopback, and SVIs for all nodes in a cluster.
- If the **rbridge-id** option is not used, information about physical, loopback, and SVIs is shown for the local node only.
- Note the following with respect to the **show ip interface loopback** command:
- The command **show ip interface loopback rbridge-id rbridge-id** shows the details of loopback interfaces for the given *rbridge-id*.
- The command **show ip interface loopback rbridge-id all** shows the details of loopback interfaces for all nodes in a cluster.
- If the **rbridge-id** option is not used, information about loopback interfaces is shown for the local node only.

Note the following with respect to the **show ip interface ve** command:

- The command **show ip interface ve rbridge-id rbridge-id** provides information about SVIs specific to the given *rbridge-id*.
- The command **show ip interface ve rbridge-id all** provides information about SVIs for all nodes in a cluster.

If the **rbridge-id** option is not used, information about SVIs is shown for the local node only. On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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
Ten Gigabit Ethernet 1/0/0              unassigned      up              up
Ten Gigabit Ethernet 1/0/1              unassigned      up              down
Ten Gigabit Ethernet 1/0/2              unassigned      up              up
Ten Gigabit Ethernet 1/0/3              unassigned      up              up
Ten Gigabit Ethernet 1/0/4              unassigned      up              down
Ten Gigabit Ethernet 1/0/5              unassigned      up              down
Ten Gigabit Ethernet 1/0/6              unassigned      up              down
Ten Gigabit Ethernet 1/0/7              unassigned      up              up
Ten Gigabit Ethernet 1/0/8              unassigned      up              up
```

```

Ten Gigabit Ethernet 1/0/9   unassigned   up           up
Ten Gigabit Ethernet 1/0/10  unassigned   up           down
Ten Gigabit Ethernet 1/0/11  unassigned   up           down
Ten Gigabit Ethernet 1/0/12  unassigned   up           up
Ten Gigabit Ethernet 1/0/13  unassigned   up           up
Ten Gigabit Ethernet 1/0/14  unassigned   up           down
Ten Gigabit Ethernet 1/0/15  unassigned   up           up
Ten Gigabit Ethernet 1/0/16  unassigned   up           down
Ten Gigabit Ethernet 1/0/17  unassigned   up           up
Ten Gigabit Ethernet 1/0/18  unassigned   up           down
Ten Gigabit Ethernet 1/0/19  unassigned   up           up
Ten Gigabit Ethernet 1/0/20  unassigned   up           up
Ten Gigabit Ethernet 1/0/21  unassigned   up           up
Ten Gigabit Ethernet 1/0/22  unassigned   up           up
Ten Gigabit Ethernet 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 port-security status when the port-security feature is applied:

```

sw0# show ip interface brief
Interface                IP-Address      Status Protocol
=====
Port-channel 1           unassigned      up    up
TenGigabitEthernet 0/1   unassigned      up    up
TenGigabitEthernet 0/2   unassigned      admin-down down  "Port security violation"
TenGigabitEthernet 0/3   unassigned      admin-down down
TenGigabitEthernet 0/4   unassigned      admin-down down  "Port security violation"

```

To display the IP interface status of a 1-gigabit Ethernet port on a Brocade VDX 6710 switch:

```

switch# show ip interface gigabitethernet 1/0/1
Gigabit Ethernet 1/0/1 is up protocol is up
    IP unassigned
    Proxy Arp is not Enabled
    ICMP unreachablees are always sent
    ICMP mask replies are never sent
    IP fast switching is enabled

```

See Also **show interface**

show ip interface loopback

Displays loopback information for a Management Cluster.

Synopsis **show ip interface loopback** *id* [**rbridge-id** *rbridge-id* | **all**]

Operands	id	Displays the information for the designated loopback.
	rbridge-id <i>rbridge-id</i>	Displays the information for the physical, loopback, and SVI interfaces specific to a given RBridge ID.
	all	Displays the information for the physical, loopback, and SVI interfaces from all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about loopbacks for switches in a management cluster.

Usage Guidelines None

Examples None

See Also **show ip interface**, **show ip interface ve**

show ip interface ve

Displays virtual Ethernet (VE) port information for a Management Cluster.

Synopsis **show ip interface ve** *id* [**rbridge-id** *rbridge-id* | **all**]

Operands	<i>id</i>	Displays the information for the designated loopback.
	rbridge-id <i>rbridge-id</i>	Displays the information for the physical, loopback, and SVI interfaces specific to a given RBridge ID.
	all	Displays the information for the physical, loopback, and SVI interfaces from all nodes in a VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about VE ports for switches in a Management Cluster.

Usage Guidelines None

Examples None

See Also **show ip interface**, **show ip interface loopback**

show ip ospf

Displays the OSPF state.

Synopsis **show ip ospf** [**vrf name** [**rbridge-id** {*rbridge-id* | **all**}]]

Operands **vrf name** Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id *rbridge-id* Displays the information for the selected RBridge.

all Displays information for all RBridges.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the OSPF state.

Usage Guidelines When the RBridge ID is not specified, the output from the local node is displayed.

When the RBridge ID is specified, data from the corresponding specified RBridge is displayed.

When **all** is specified, data from all nodes in the cluster is displayed.

Examples

```
Switch# show ip ospf vrf testname
OSPF Version                Version 2
Router Id                   0.0.0.0
ASBR Status                 No
ABR Status                  No          (0)
Redistribute Ext Routes from
Initial SPF schedule delay  0          (msecs)
Minimum hold time for SPF  5000        (msecs)
Maximum hold time for SPF  10000       (msecs)
External LSA Counter        0
External LSA Checksum Sum   0
Originate New LSA Counter   0
Rx New LSA Counter          0
External LSA Limit          14913080
Database Overflow Interval   0
Database Overflow State :   NOT OVERFLOWED
RFC 1583 Compatibility :   Enabled
NSSA Translator:            Enabled
Nonstop Routing:            Disabled
Originating router-LSAs with maximum metric
Condition: Always Current State: Active
Link Type: TRANSIT
Additional LSAs originated with maximum metric:
LSA Type                    Metric Value
AS-External                 16711680
Type 3 Summary              16711680
Type 4 Summary              16711680
```

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*]] [[**vrf** *vrfname* [**rbridge-id** [*rbridge-id* | **all**]]] | **rbridge-id** [*rbridge-id* | **all**]]

Operands	<i>A.B.C.D</i>	Area address in dotted decimal format.
	<i>decimal</i>	Area address in decimal format. Valid values range from 0 to 2147483647.
	database link-state	Displays database link-state information.
	advertise <i>index</i>	Displays the link state by Link State Advertisement (LSA) index.
	asbr	Displays the link state for all autonomous system boundary router (ASBR) links.
	<i>asbrid</i>	Displays the state of a single ASBR link that you specify.
	adv-router <i>rid</i>	Displays the link state for the advertising router that you specify.
	extensive	Displays detailed information for all entries in the OSPF database.
	link-state-id <i>lid</i>	Displays the link state by link-state ID.
	network	Displays the link state by network link.
	<i>netid</i>	Displays the link state of a particular network link that you specify.
	adv-router <i>rid</i>	Displays the link state by the advertising router that you specify.
	nssa	Displays the link state by not-so-stubby area (NSSA).
	<i>nsaaid</i>	Displays the link state of a particular NSAA area that you specify.
	adv-router <i>rid</i>	Displays the link state for the advertising router that you specify.
	router	Displays the link state by router link.
	<i>routerid</i>	Displays the link state of a particular router link that you specify.
	adv-router <i>rid</i>	Displays the link state by the advertising router that you specify.
	router-id <i>rid</i>	Displays the link state by advertising router that you specify.
	self-originate	Displays self-originated link states.
	sequence-number <i>num</i>	Displays the link-state by sequence number that you specify.
	summary	Displays the link state summary. Can specify link-state ID or advertising router ID.
	adv-router <i>rid</i>	Displays the link state for the advertising router that you specify.
	vrf <i>vrfname</i>	Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.
	rbridge-id <i>rbridge-id</i>	Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

2 show ip ospf area

all Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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] [[vrf vrfname [rbridge-id {rbridge-id | all}]] | rbridge-id {rbridge-id | all}]

Operands

A.B.C.D	Specifies the router ID in dotted decimal format.
vrf vrfname	Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.
rbridge-id rbridge-id	Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.
all	Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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.

Usage Guidelines None

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** [[vrf vrfname [rbridge-id {rbridge-id | all}]] | rbridge-id {rbridge-id | all}]

Operands **vrf vrfname** Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id rbridge-id Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

all Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about the OSPF configuration.

Usage Guidelines None

Examples

```
switch# 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: 14913080
OSPF Database Overflow Interval: 0
RFC 1583 Compatibility: Enabled
Router id: 0.0.0.0
OSPF Area currently defined:
Area-ID          Area-Type Cost
0                 normal  0
1                 normal  0

OSPF Area Range currently defined:
Area-ID  Range-Address  Subnetmask  Status  Config-Cost
1        20.0.0.0    255.0.0.0   advertise 100
1        30.0.0.0    255.0.0.0   not-advertise -
```

See Also None

show ip ospf database

Shows database information.

Synopsis	show ip ospf database [[vrf <i>vrfname</i> [rbridge-id { <i>rbridge-id</i> all}]] rbridge-id { <i>rbridge-id</i> all}	
	show ip ospf database database-summary [[vrf <i>vrfname</i> [rbridge-id { <i>rbridge-id</i> all}]] rbridge-id { <i>rbridge-id</i> all}	
	show ip ospf database external-link-state [advertise <i>index</i> extensive link-state-id <i>lid</i> router-id <i>routerid</i> sequence-number <i>num</i>] [[vrf <i>vrfname</i> [rbridge-id { <i>rbridge-id</i> all}]] rbridge-id { <i>rbridge-id</i> all}	
	show ip ospf database link-state [advertise <i>index</i> asbr { <i>asbrid</i> adv-router <i>rid</i> } extensive link-state-id <i>lid</i> network { <i>netid</i> adv-router <i>rid</i> } nssa { <i>nsaaid</i> adv-router <i>rid</i> } router [{ <i>routerid</i> adv-router <i>rid</i> } router-id <i>routerid</i> self-originate sequence-number <i>num</i> summary { <i>lid</i> adv-router <i>rid</i> }]	
Operands	database-summary	Displays how many link state advertisements (LSAs) of each type exist for each area, as well as total number of LSAs.
	external-link-state	Displays information by external link state, based on the following parameters:
	advertise <i>index</i>	Displays the hexadecimal data in the specified LSA packet. The <i>index</i> 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	Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.
	link-state-id <i>lid</i>	Displays external LSAs for the LSA source that you specify.
	router-id <i>routerid</i>	Displays external LSAs for the advertising router that you specify.
	sequence-number <i>num</i>	Displays the External LSA entries for the hexadecimal LSA sequence number that you specify.
	link-state	Displays the link state, based on the following parameters:
	advertise <i>index</i>	Displays the hexadecimal data in the specified LSA packet. The <i>index</i> 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	Displays autonomous system boundary router (ASBR) LSAs.
	extensive	Displays LSAs in decrypt format. Do not use this parameter in combination with other display parameters because the entire database is displayed.
	link-state-id <i>lid</i>	Displays LSAs for the LSA source that you specify.
	network	Displays either all network LSAs or the LSAs for a network that you specify.
	nssa	Displays either all NSSA LSAs or the LSAs for a not-so-stubby area (NSSA) that you specify.
	router	Displays LSAs by router link.

router-id <i>routerid</i>	Displays LSAs for the advertising router that you specify.
self-originate	Displays self-originated LSAs.
sequence-number	Displays the LSA entries for the hexadecimal LSA sequence number that you specify.
summary	Displays summary information. You can specify link-state ID or advertising router ID.
adv-router <i>rid</i>	Displays the link state for the advertising router that you specify.
vrf <i>name</i>	Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.
rbridge-id <i>rbridge-id</i>	Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.
all	Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display debug information based on the parameters you enable.

Usage Guidelines None

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# 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	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 <i>rbridge-id/slot/port</i> [brief] gigabitethernet <i>rbridge-id/slot/port</i> [brief] loopback <i>number</i> port-channel <i>number</i> [brief] tengigabitethernet <i>rbridge-id/slot/port</i> [brief] ve <i>vlan_id</i> [brief]}] [brief]] [[vrf <i>vrfname</i> [rbridge-id {rbridge-id all}]] rbridge-id {rbridge-id all}]]	
Operands	A.B.C.D	Specifies interface IP address in dotted decimal format.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet port interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This parameter is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	brief	Displays brief summary information about the specified port.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	brief	Displays brief summary information about the specified port.
	loopback <i>number</i>	Specifies a loopback port number in the range of 1 to 255.
	port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
	brief	Displays brief summary information about the specified port channel.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	brief	Displays brief summary information about the specified port.
	ve <i>vlan_id</i>	Specifies the VLAN number.
	brief	Displays brief summary information about the specified VLAN.
	brief	Displays brief summary about all enabled interfaces.
	vrf <i>vrfname</i>	Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.
	rbridge-id <i>rbridge-id</i>	Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

	all	Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to display information about all or specific OSPF-enabled interfaces.	
Usage Guidelines	If the physical interface type and name are specified, the rbridge-id option is not available.	
Examples	To display information about all enabled interfaces: switch# show ip ospf interface TenGigabitEthernet 3/0/1 admin up, oper up IP Address 100.1.1.1, Area 0 Database Filter: Not Configured State passive(default none), Pri 1, Cost 1, Options 2, Type broadcast Events 0 Timers(sec): Transmit 1, Retrans 5, Hello 10, Dead 40 DR: Router ID 0.0.0.0 Interface Address 0.0.0.0 BDR: Router ID 0.0.0.0 Interface Address 0.0.0.0 Neighbor Count = 0, Adjacent Neighbor Count= 0 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 <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i> loopback <i>number</i> port-channel <i>number</i> router-id <i>A.B.C.D</i> tengigabitethernet <i>rbridge-id/slot/port</i> ve <i>vlan_id</i> } [[vrf <i>vrfname</i> [rbridge-id { <i>rbridge-id</i> all }}] rbridge-id { <i>rbridge-id</i> all }]	
Operands	extensive	Shows detailed information about all neighbors.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Show neighbor information for the specified, valid 40-gigabit Ethernet port interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This parameter is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Displays neighbor information for the specified, valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	loopback <i>number</i>	Specifies a loopback port number in the range from 1 through 255.
	port-channel <i>number</i>	Displays neighbor information for the specified, valid port-channel number. Valid values range from 1 through 6144.
	router-id <i>A.B.C.D</i>	Displays neighbor information for the specified router ID (in dotted decimal format).
	tengigabitethernet <i>rbridge-id/slot/port</i>	Displays neighbor information for the specified, valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	ve <i>vlan_id</i>	Specifies a virtual Ethernet (VE) interface. Refer to the Usage Guidelines.
	vrf <i>vrfname</i>	Specifies the name of the VRF instance. If this option is not used, details for the default VRF instance are shown in the output.
	rbridge-id <i>rbridge-id</i>	Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.
	all	Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults	None																		
Command Modes	Privileged EXEC mode																		
Description	Use this command to display information about OSPF neighbors.																		
Usage Guidelines	If the physical interface type and name are specified, the rbridge-id option is not available. On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.																		
Examples	To show information about all OSPF neighbors: <pre>switch# show ip ospf neighbor Number of Neighbors is 2, in FULL state 1</pre> <table><tr><th>Port</th><th>Address</th><th>Pri</th><th>State</th><th>Neigh Address</th><th>Neigh ID</th><th>Ev</th><th>Opt</th><th>Cnt</th></tr><tr><td>2/2</td><td>22.22.22.1</td><td>0</td><td>FULL/OTHER</td><td>22.22.22.2</td><td>192.0.0.1</td><td>5</td><td>2</td><td>0</td></tr></table>	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
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 redistribute route

Displays redistributed routes.

Synopsis **show ip ospf redistribute route** [A.B.C.D:M] [[vrf vrfname [rbridge-id {rbridge-id | all}]] | rbridge-id {rbridge-id | all}]

Operands	A.B.C.D:M	Specifies an IP address and mask for the output.
	vrf vrfname	Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.
	rbridge-id rbridge-id	Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.
	all	Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display routes that have been redistributed into OSPF.

Usage Guidelines None

Examples switch# **show ip ospf redistribute route**
30.30.30.0 255.255.255.0 fwd 0.0.0.0 (0) metric 10 connected
50.1.0.0 255.255.0.0 fwd 100.1.1.100 (1) metric 10 static

See Also None

show ip ospf routes

Displays routes.

Synopsis **show ip ospf routes** [*A.B.C.D*] **[[vrf** *vrfname* **[rbridge-id** {*rbridge-id* | **all**}]] **| rbridge-id** {*rbridge-id* | **all**}]

Operands

<i>A.B.C.D</i>	Specifies a destination IP address in dotted decimal format.
vrf <i>vrfname</i>	Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.
rbridge-id <i>rbridge-id</i>	Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.
all	Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display routes that OSPF calculated. You can display all routes or you can display information about a specific route.

Usage Guidelines None

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** *[[vrf vrfname [rbridge-id {rbridge-id | all}]] | rbridge-id {rbridge-id | all}]*

Operands **vrf vrfname** Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.

rbridge-id rbridge-id Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.

all Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display summary information for all OSPF instances.

Usage Guidelines None

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 <i>rbridge-id/slot/port</i> gigabitethernet <i>rbridge-id/slot/port</i> loopback <i>number</i> port-channel <i>number</i> tengigabitethernet <i>rbridge-id/slot/port</i> ve <i>vlan_id</i>]] [[vrf <i>vrfname</i> [rbridge-id { <i>rbridge-id</i> all }]] rbridge-id { <i>rbridge-id</i> all }]	
Operands	fortygigabitethernet <i>rbridge-id/slot/port</i>	Displays traffic information for the specified, valid 40 Gbps port interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This parameter is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Displays traffic information for the specified, valid 1-gigabit Ethernet interface
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	loopback <i>number</i>	Specifies a loopback port number in the range from 1 through 255.
	port-channel <i>number</i>	Specifies the interface is a port-channel. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Displays traffic information for the specified, valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	ve <i>vlan_id</i>	Specifies a virtual Ethernet (VE) interface. Refer to the Usage Guidelines.
	vrf <i>vrfname</i>	Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.
	rbridge-id <i>rbridge-id</i>	Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.
	all	Displays the information for the physical, loopback, and SVI interfaces of all nodes in cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.
Defaults	None	
Command Modes	Privileged EXEC mode	

2 show ip ospf traffic

Description Use this command to display details of OSPF traffic sent and received. You can display all traffic or specify a particular interface.

Usage Guidelines If the physical interface type and name are specified, the rbridge-id option is not available.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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!
```

See Also None

show ip ospf virtual

Displays information about virtual links.

Synopsis **show ip ospf virtual** {link | neighbor} [index] [[vrf vrfname [rbridge-id {rbridge-id | all}]] | rbridge-id {rbridge-id | all}]

Operands

link <i>index</i>	Shows information about all virtual links or one virtual link that you specify.
neighbor <i>index</i>	Shows information about all virtual neighbors or one virtual neighbor that you specify.
vrf <i>vrfname</i>	Specifies the name of the VRF instance. If this option is not used, details for the default VRF are shown in the output.
rbridge-id <i>rbridge-id</i>	Displays the information for the physical, loopback, and SVI interfaces specific to the selected RBridge.
all	Displays the information for the physical, loopback, and SVI interfaces of all nodes in the VCS cluster. There can be multiple loopbacks and SVIs with the same RBridge ID from different nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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.

Usage Guidelines None

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 pim bsr

Displays the Boot Strap Router (BSR) information.

Synopsis **show ip pim bsr** [**rbridge-id** *rbridge-id*]

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the BSR information. The information displayed ignores whether the Protocol Independent Multicast router is the elected BSR or not.

Usage Guidelines None

Examples A typical output for this command.

```
switch# show ip pim bsr
```

```
PIMv2 Bootstrap information :
```

```
-----  
BSR address: 10.10.10.1. Hash Mask Length 32. Priority 0.
```

See Also router pim, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim group

Displays the list of multicast groups.

Synopsis **show ip pim group** [**rbridge-id** *rbridge-id*]

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display a list of the multicast groups that Protocol Independent Multicast (PIM) has learned. All groups, irrespective of how PIM learned them, are displayed.

Usage Guidelines None

Examples A typical output for this command.

```
switch# show ip pim group
Total number of groups: 2
1      Group 225.0.0.1
      Group member at   Te 19/2/1: Te 19/2/1
      Group member at   Ve 100: Ve 100
2      Group 225.0.0.2
      Group member at   Te 19/2/1: Te 19/2/1
      Group member at   Ve 100: Ve 100
```

See Also router pim, show ip pim bsr, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim mcache

Displays the multicast cache.

Synopsis	show ip pim mcache [<i>ip-address-1</i> [<i>ip-address-2</i>]] [rbridge-id <i>rbridge-id</i>]
Operands	<i>ip-address-1</i> Group/Source IP address <i>ip-address-2</i> Group/Source IP address rbridge-id <i>rbridge-id</i> Specifies the RBridge ID.
Defaults	None
Command Modes	Privileged EXEC mode
Description	Use this command to display the entries in the multicast cache.
Usage Guidelines	None
Examples	A typical output for this command. <pre> switch# show ip pim mcache 231.0.0.10 IP Multicast Mcache TableEntry Flags : sm - Sparse Mode, ssm - Source Specific Multicast RPT - RPT Bit, SPT - SPT Bit, LSrc - Local Source LRcv - Local Receiver, RegProbe - Register In Progress RegSupp - Register Suppression Timer, Reg - Register Complete L2Reg - L2 Registration, needRte - Route Required for Src/RPTotal entries in mcache: 2001 (*, 231.0.0.10) RP 22.22.22.22 in Te 18/0/5, Uptime 00:00:56 Sparse Mode, RPT=1 SPT=0 Reg=0 L2Reg=0 RegSupp=0 RegProbe=0 LSrc=0 LRcv=1 upstream neighbor=13.13.13.1 num_oifs = 1 Ve 10, Ve 10(00:00:56/0) Flags (0x012604a0) sm=1 ssm=0 needRte=02 (14.14.14.100, 231.0.0.10) in Te 18/0/1, Uptime 00:00:31 Sparse Mode, RPT=0 SPT=0 Reg=0 L2Reg=0 RegSupp=0 RegProbe=0 LSrc=0 LRcv=1 upstream neighbor=48.48.48.5 num_oifs = 1 Ve 10, Ve 10(00:00:31/0) Flags (0x010600f5) sm=1 ssm=0 needRte=0Number of matching entries: 2 </pre>
See Also	router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic

show ip pim neighbor

Displays the Protocol Independent Multicast (PIM) neighbor information.

Synopsis **show ip pim neighbor** [**rbridge-id** *rbridge-id*]

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about all the neighbors that the PIM router perceives as active.

Usage Guidelines None

Examples A typical output for this command.

```
switch# show ip pim neighbor
Total Number of Neighbors : 43
Port          Phy_Port      Neighbor      Holdtime    Age    UpTime        Priority
              sec          sec          Dd HH:MM:SS
Te 125/1/31    Te 125/1/31    125.31.1.1    105         0      00:29:30      1
Te 125/1/43    Te 125/1/43    125.49.43.2    105         20     00:29:30      1
Te 125/2/1     Te 125/2/1     125.2.1.2     105         10     00:29:40      1
Ve 2000        Ve 2000        10.1.1.5      105         0      00:27:00      1
Ve 2001        Ve 2001        21.1.1.3      105         0      00:27:00      1
Ve 2002        Ve 2002        22.1.1.131    105         0      00:27:00      1
```

See Also router pim, show ip pim bsr, show ip pim group, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim rpf

Displays the Reverse Path Forwarding (RPF) for a given unicast IP address.

Synopsis **show ip pim rpf** *A.B.C.D*

Operands *A.B.C.D* The unicast IP address.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the port that PIM regards as the best reverse path for a given unicast IP address.

Usage Guidelines The unicast IP address may be an RP address or source address.

Examples A typical output for this command.

```
switch# show ip pim rpf 123.32.120.10  
Source 123.32.120.10 directly connected on Te 1/0/21
```

See Also router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim rp-hash

Displays the Rendezvous Point (RP) information for a Protocol Independent Multicast (PIM) sparse group.

Synopsis **show ip pim rp-hash** *A.B.C.D*

Operands *A.B.C.D* Group address in dotted decimal format.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the RP information for a PIM sparse group. It displays all RPs for the given group. The RP address could have been learned either from the Boot Strap Router (BSR) or configured statically.

Usage Guidelines None

Examples A typical output for this command.

```
switch# show ip pim rp-hash 225.125.1.1  
RP: 10.10.10.1, v2
```

See Also router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim rp-map

Displays the Rendezvous Point (RP) to group mappings.

Synopsis **show ip pim rp-map** [**rbridge-id** *rbridge-id*]

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the RP to group mappings.

Usage Guidelines None

Examples A typical output for this command.

```
switch# show ip pim rp-map
Number of group-to-RP mappings: 6
Group address RP address
-----
1 239.255.163.1 99.99.99.5
2 239.255.163.2 99.99.99.5
3 239.255.163.3 99.99.99.5
4 239.255.162.1 99.99.99.5
5 239.255.162.2 43.43.43.1
6 239.255.162.3 99.99.99.5
```

See Also router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim rp-set

Displays the Rendezvous Point (RP) set list.

Synopsis **show ip pim rp-set** [**rbridge-id** *rbridge-id*]

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information regarding all RPs that Protocol Independent Multicast (PIM) perceives. The RPs may be either statically or dynamically learned.

Usage Guidelines None

Examples A typical output for this command.

```
switch# show ip pim rp-set
```

```
Static RP
```

```
-----
```

```
Static RP count: 1
```

```
RP: 22.22.22.22
```

```
Number of group prefixes Learnt from BSR: 1
```

```
Group prefix = 231.0.0.0/4      # RPs expected: 1
```

```
# RPs received: 1
```

```
RP 1: 33.33.33.33    priority=0    age=10    holdtime=150
```

```
switch#
```

See Also router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim-sparse, show ip pim traffic, show ip pim traffic, show ip pim traffic

show ip pim-sparse

Displays the Protocol Independent Multicast (PIM) router parameters.

Synopsis **show ip pim-sparse** [**interface** {**tengigabitethernet** *rbridge-id* /*slot*/*port* | **gigabitethernet** *rbridge-id*/*slot*/*port* | **fortygigabitethernet** *rbridge-id* /*slot*/*port* | **ve** *vlan_id*}]

Operands **tengigabitethernet** *rbridge-id*/*slot*/*port*
 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id*/*slot*/*port*
 Specifies a valid 1-gigabit Ethernet interface

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

fortygigabitethernet *rbridge-id*/*slot*/*port*
 Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID. This is not valid in standalone mode.

slot Specifies a valid slot number.

port Specifies a valid port number.

ve *vlan_id* Specifies a virtual Ethernet (VE) interface. Refer to the Usage Guidelines.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the internal parameters of the PIM router. It also displays the parameters of the PIM enabled interface.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples A typical output for this command.

```
switch# show ip pim-sparse
Global PIM Sparse Mode settings
Maximum mcache: 2048 Current count: 0
Hello interval: 30 Neighbor timeout: 105
```

Join/Prune interval: 60 Inactivity interval: 180
Hardware drop enabled: Yes Prune wait interval: 3
Bootstrap Msg interval: 60 Candidate-RP Msg interval: 60
Register Suppress Time: 60 Register Probe Time: 10
Register Stop Delay: 60 Register Suppress interval: 60
SSM Enabled: No SPT Threshold: 1

Interface	Local Address	Ver	Mode	Designated Router Address Port	TTL Thr	Multicast Boundary	VRF	DR Prio
Te 1/0/15	12.12.12.12	v2	SM	Itself	1	None	0	1

See Also router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim traffic, show ip pim traffic, show ip pim traffic

2 show ip pim traffic

show ip pim traffic

Displays the Protocol Independent Multicast (PIM) traffic statistics.

Synopsis **show ip pim traffic** [**rbridge-id** *rbridge-id*]

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display PIM traffic statistics, categorized by each PIM enabled interface.

Usage Guidelines None

Examples None

See Also router pim, show ip pim bsr, show ip pim group, show ip pim neighbor, show ip pim rpf, show ip pim rp-hash, show ip pim rp-map, show ip pim rp-set, show ip pim-sparse, show ip pim traffic, show ip pim traffic

show ip route

Shows IP route information.

Synopsis **show ip route**

show ip route *A.B.C.D/M* [**debug** | **detail** | **longer**]

show ip route [**all**] [**connected**] [**ospf**] [**bgp**] [**slot** *line_card_number*] [**static**] [**summary**] [**vrf** *name*] [**rbridge-id** *rbridge-id*]

show ip route nexthop [*nexthopID*] [**ref-routes**]

Operands	<i>A.B.C.D/M</i>	Specifies the IPv4 address/length to show information for a specific route.
	debug	Displays debug information.
	detail	Displays more-specific routes with the same specified prefix.
	longer	Displays routes with addresses that match the address/mask prefix.
	rbridge-id	Displays routes for a selected RBridge ID.
	vrf	Displays routes for a selected VRF instance.
	all	Displays information for all configured ip routes.
	bgp	Displays BGP route information.
	connected	Displays directly connected routes, such as local Layer 3 interfaces.
	nexthop	Displays information about the configured next hop.
	<i>nexthopID</i>	Valid values range from 0 through 65535.
	ref-routes	Displays all routes that point to the specified <i>nexthopID</i> .
	ospf	Displays routes learned from the Open Shortest Path First (OSPF) protocol.
	rbridge-id <i>rbridge-id</i>	Displays routes for a selected RBridge ID.
	slot <i>line_card_number</i>	Displays information for routes with the provided line card number.
	static	Displays information about the configured static routes.
	summary	Displays summary information for all routes.
	vrf <i>name</i>	Displays routes for a selected VRF instance.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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
```

2 show ip route

```

      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

switch(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

switch(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

```

See Also None

2 show ipv6 route

show ipv6 route

Displays the IPv6 route information.

Synopsis **show lipv6 route**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the IPv6 route information.

Usage Guidelines None

Examples None

See Also None

show lacp

Displays Link Aggregation Control Protocol (LACP) statistics.

Synopsis **show lacp** [**counters** [*port-channel*] | **sys-id** [*port-channel*]]

Operands	counters	Displays LACP statistics for all port-channel interfaces.
	<i>port-channel</i>	Displays counters for a specified port channel interface. Valid values range from 1 through 6144.
	sys-id	Displays LACP statistics by system ID.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the LACP statistics for each port-channel interface for all port-channel interfaces or a single port-channel interface, or by system ID.

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** {*rbridge-id ID* | **all**}] [**all**]

Operands

rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
<i>rbridge-id</i>	Specifies a unique identifier for a node.
all	Specifies all identifiers for a node.
all	Executes the command on all switches in the fabric.

Defaults 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, the feature name, and an indication of whether the license is valid. A string of “x” characters is displayed for the license key.

Usage Guidelines In the Network OS v3.0.0 release, use this command to display only the licenses installed on the local RBridge.

In logical chassis cluster mode, remote license operations may be performed on any remote RBridge, from any RBridge in the logical chassis cluster.

Examples To display license information on a Brocade VDX 6720-60 switch:

```
switch# show license
Rbridge-Id: 2
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    FCoE Base license
    Feature name:FCOE_BASE    License is valid
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    First Ports on Demand license - additional 10 port upgrade license
    Feature name:PORTS_ON_DEMAND_1
    License is valid
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    Second Ports on Demand license - additional 10 port upgrade license
    Feature name:PORTS_ON_DEMAND_2
    License is valid
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
```

To display a Brocade VDX 8770 licensed for Advanced Services: (This configuration enables the use of Layer 3 and FCoE features. The VCS Fabric license is enabled on all VDX platforms by default starting with Network OS 4.1.0; a VCS Fabric license does not need to be installed to enable VCS Fabric functionality.)

```
switch# show license
rbridge-id: 60
xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxx
    Advanced Services license
    Feature name:ADVANCED_SERVICES
    License is valid
```

2 show license

See Also license add, license remove, show license id

show license id

Displays the RBridge License ID.

Synopsis	show license id [rbridge-id {rbridge-id all}] [all]	
Operands		
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	rbridge-id	Specifies a unique identifier for a node.
	all	Specifies all identifiers for a node.
	all	Executes the command on all switches in the fabric.
Defaults	Displays the license ID installed on the local switch.	
Command Modes	Privileged EXEC mode	
Description	Use this command to display the RBridge license ID (WWN) for the specified switch. You need the RBridge license ID when you prepare to add a license.	
Usage Guidelines	In the Network OS v3.0.0 release, this command is supported only on the local RBridge. In logical chassis cluster mode, remote license operations may be performed on any remote RBridge, from any RBridge in the logical chassis cluster.	
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 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 line cards present in a modular switch. The output includes the following information:

Slot Displays the slot number. Slots for line cards are L1 through L4 on Brocade VDX 8770-4 switches, and L1 through L8 on Brocade VDX 8770-8 switches.

Type Displays the line card type.

Description Module description

ID Displays IDs for line cards.

Status Displays the status of the line card 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).

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 line cards present in a Brocade VDX 8770-4 switch:

```
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 rbridge-id/slot/port		
		Specifies a valid 10-gigabit Ethernet interface.	
	rbridge-id	Specifies the RBridge ID.	
	slot	Specifies a valid slot number.	
	port	Specifies a valid port number.	
	gigabitethernet rbridge-id/slot/port		
		Specifies a valid 1-gigabit Ethernet interface.	
	rbridge-id	Specifies the 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 LLDP status on the specified interface.		
Usage Guidelines	The gigabitethernet rbridge-id/slot/port parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.		
Examples	To display all the LLDP interface information for a selected interface:		
	<pre>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 tengigabitethernet 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</pre>		
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** Specifies an Ethernet interface.

tengigabitethernet *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

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.

ATTENTION

If you do not use the **interface** parameter, only the mandatory TLVs are displayed.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

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
```

2 show lldp neighbors

```
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** Specifies an Ethernet interface.

tengigabitethernet *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the 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 LLDP statistics on all interfaces or a specified interface.

If you do not specify an interface, Use this command to display the LLDP statistics for all interfaces.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

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* | **all**]

Operands	reverse	Displays the audit log in reverse order.
	rbridge-id	Executes the command on the specified switch.
	<i>rbridge-id</i>	Specifies the RBridge ID for the switch.
	all	Executes the command on all switches in the fabric.

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, log-dampening-debug (BGP)**

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 <i>attribute</i>	Filters output by message attribute. Valid attributes include FFDC and VCS.
blade <i>blade</i>	Displays for the specified blade only. Valid values for blade include MM1, MM2, and LC[1-8].
count <i>count</i>	Specifies the number of messages to display.
message-type <i>type</i>	Filters the output by message type. Valid message types include DCE or SYSTEM.
severity <i>severity</i>	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 <i>rbridge-id</i>	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)
```

2 show logging raslog

To display all RASLog messages for a line card:

```
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
```

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** {**fortygigabitethernet** *rbridge-id/slot/port* | **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-addr*

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.

fortygigabitethernet *rbridge-id/slot/port*

Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*

Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*

Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

port-channel *number*

Specifies the port-channel number. Valid values range from 1 through 63.

linecard interface Displays the forwarding information for a line card interface.

tengigabitethernet *rbridge-id/slot/port*

Specifies a valid 10-gigabit Ethernet line-card interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

2 show mac-address-table

<i>port</i>	Specifies a valid port number.
gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet line-card interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
static	Displays the static MAC addresses.
vlan <i>vlan_id</i>	Specifies the VLAN number. Refer to the Usage Guidelines.
port-profile	Displays MAC addresses associated with port profiles.
address <i>mac-address</i>	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 <i>vlan_id</i>	Displays MAC addresses associated with port profiles and the specified VLAN. Refer to Usage Guidelines below.

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* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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	The TX Power Field in the show media command is not supported by the 40-Gbps optics.
Examples	To display all SFP information:

```
switch# show media
Interface Ten Gigabit Ethernet 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** *rbridge-id/slot/port*
 Specifies a valid external 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid external 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

fibrechannel *rbridge-id/slot/port*
 Specifies a valid external 1-gigabit FibreChannel interface.

rbridge-id Specifies the 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 a summary of the SFP information for the specified interface.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

The **fibrechannel** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6730 switches.

Examples To display SPF information for a 1-gigabit Ethernet interface:

```
switch# show media interface gigabitethernet 1/0/1
Interface      Gigabit Ethernet 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
```

2 show media interface

```
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-gigabit Ethernet interface:

```
switch# show media interface tengigabitethernet 5/0/1
Interface Ten Gigabit Ethernet 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 line card.

Synopsis **show media linecard** *number*

Operands *number* Numeric identifier for the line card.

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 line card in slot 2:

```
switch# show media linecard 2
Interface      Ten Gigabit Ethernet 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 Quad SFP media information for an LC12X40G line card 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 line card 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-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.		
	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 name-server brief

Displays brief entries of local name server (NS) information about devices connected to a switch.

Synopsis	show name-server brief [<i>rbridge-id</i> <i>rbridge-id</i>]	
Operands	rbridge-id <i>rbridge-id</i>	Specifies the RBridge ID of the switch for which the brief name server entries are displayed.
Defaults	If no RBridge ID is specified, brief entries for all devices in the fabric are displayed.	
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.	
	NOTE	
	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 ID of the switch for which the details about name server entries are displayed.

Defaults If no RBridge ID is specified, detailed entries for all devices in the fabric are displayed.

Command Modes Privileged EXEC mode

Description Use this command to display 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

2 show name-server detail

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.

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 World Wide Name (WWN) 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. The lookup is performed using either the Fibre Channel address (Port ID, or PID), or the WWN of the device. 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

Refer to **show name-server detail** for descriptions of the displayed information.

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 <i>pid</i> WWN <i>wwn</i>}	
Operands	PID <i>pid</i>	Specifies the Fibre Channel address of the device.
	WWN <i>wwn</i>	Specifies the World Wide Name (WWN) 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 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: <i>Device with PID of pid does not exist</i> • For WWN lookup: <i>Device with WWN of wwn does not exist</i>	
Examples	To view name server information for a device specified by PID:	
	<pre> 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 </pre>	

See Also show name-server brief, show name-server detail, show name-server nodefind

show nas statistics

Displays automatic network attached storage (Auto NAS)) statistics.

Synopsis **show nas statistics all** | **server-ip** *ip_addr/prefix* [**vlan** *VLAN_id* | **vrf** *VRF_name*] [**rbridge-id** *rbridge-id*]

Operands **all** Shows all gathered statistics.

server-ip IP address to show Auto NAS statistics for.

ip_addr/prefix IPv4 address/prefix of a specified Auto NAS port.

vlan *VLAN_id* Specifies which VLAN interface to display the statistics for.

vrf *VRF_name* Specifies which VRF interface to display the statistics for.

rbridge-id *rbridge-id* Specifies which RBridge ID to display the statistics for.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the specified Auto NAS server statistics.

Usage Guidelines This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Examples None

See Also **backup-advertisement-interval, clear nas statistics, nas auto-qos, nas server-ip, show running-config nas server-ip, show system internal nas, show cee maps**

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 mode

Description Use this command to display 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 advertised 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 Use this command to display 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 Use this command to display 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 Use this command to display 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 Use this command to display the following information about each active NETCONF session:

- Transport used by the session
- Login name of the user
- Client IP address
- The time 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 Use this command to display 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 notification stream

Displays notifications about the event stream.

Synopsis **show notification stream**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display notifications about the event stream.

Usage Guidelines None

Examples None

See Also None

show nsx controller

Displays connection status and statistics for the NSX controller.

Synopsis `show nsx-controller [ brief | client-cert | name name ]`

Operands

brief	Shows a brief listing of NSX controller connections.
client-cert	Displays the public certificate used for the NSX controller connection.
name <i>name</i>	Displays the name of the NSX controller profile that has been configured.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the connection state and statistics for the NSX controller. Possible states are shown in the table below.

TABLE 1 NSX controller connection states

State	Meaning
Connected	Connection is up and operational.
Not activated	User has shut down the connection.
Connection in progress	Switch is attempting to connect to the NSX controller.
Connection lost	Disconnected by peer, or network reachability has been lost. The switch will automatically attempt to connect after the configured amount of reconnect-interval seconds.
Connection dead	Switch could not connect to the NSX controller after the maximum number of reconnect attempts. The user can restart the connection via the "nsx-controller reconnect" command (Privileged EXEC mode) or via the "no activate" and "activate" commands in NSX Controller configuration mode.

Usage Guidelines This command is available only for a switch that is in logical chassis cluster mode.

Examples Example 1

To show the status of the NSX controller:

```
sw0# show nsx-controller
```

```
NSX controller cluster "yy"
Seed IP address 192.168.0.13, port 6632, method SSL
Reconnect interval 10 secs, Max retries 100
Admin state up, Number of connections 1
Number of tunnels 2, Number of MACs 4
Connection details:
  ID fb580822-b185-4068-8c9b-f15a800b4eea, Connected
  IP address 192.168.0.13, port 6632, method SSL
  Reconnect interval 10000 millis, Number of retries 0 (max 100)
  Last connect time: Wed Jan 29 16:33:48 2014
  Last disconnect time: Wed Jan 29 16:33:48 2014
```

Example 2

To show a brief listing of NSX controller connections:

```
sw0# show nsx-controller brief
```

Controller name	IP address	Port	Type	Connection state
yy	192.168.0.13	6632	SSL	Connected

Example 3

To display the public certificate used for the NSX controller connection:

```
sw0# show nsx-controller client-cert
```

```
-----BEGIN CERTIFICATE-----
MIIC2jCCAcICAQEwDQYJKoZIhvcNAQEFBQAwMzELMAkGA1UEBhMCQ0ExEDAOBgNV
BAoTB0Jyb2NhZGUxZjAQBgNVBAMTCWxvY2FsaG9zdDAeFw0xNDAxMjYxMDZa
Fw0xNTAxMjYxMDZaMDMxCzAJBgNVBAYTAkNBMR4wDgYDVQQKEwdCcm9jYWR1
MRIwEAYDVQQDEwlsb2NhbGhvc3QwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCtVSTo/ZYpA591cuSGoNRiT7mPHUzn5SUyTMM6J4ZlFETD5iLmjZbiU4
hUd45tnSYPgSxts4oArk1AobAdj1KS/Y4WuVXgQWSqQf4mLEnO5ONsazHGt+I/TV
SL4DWqfZ/SMOYpDPW326iN6I9JI0MctcDPNm49pmroAZkePxClzuAh5LakYIGsga
1/5gGWX2Gkt0Jv5inljZ43rsNpVUzylb+wTrhUbWlAFx6y6wZtAdNWz8mpoguV8E
WB7W4wolttqyAu0X8OkGOCwnyRmrG/eu4PmTkBxpOQnsHfkEtLlnbu3Nt9l6v8gKn
/0mi+tS22+2jdH9OzWMuSV0vxt5pAgMBAAEwDQYJKoZIhvcNAQEFBQADggEBABj2
rjDhCiByiwl65SODhlFy5+z8Pi/m4aCa1NH1yI9EteRC7nbYs94wu6DuJ5LaET3l
JWtKjY0aZ2Um0Sg91l3aG9+kkaVtn3oMgAre7/pRxuxssId7PuLibYqfz1zuwtwa
wVbtsrxUwZYW55mFOI7+ACMQKq3WUUb8S14vrNq+gB49kPJAQSYaygHZ+FdPYd01
j7B2L495jaXBtkttz/hai5BGqKwnfxlSqH0pI+RLrEvJrUHbwIMUNAcBODRZqxnX
0WmnxW5IIynvyRZAx6AH3EdCWjKMXA3/D8VQ/eDoYNVa65um43EsHRiPSjg/AnrO
dQDO4meBm7uFdqS4Gf0=
-----END CERTIFICATE-----
```

See Also

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	Specifies one or all RBridge IDs.
	<i>rbridge-id</i>	Specifies the RBridge ID on which the NTP server status displays.
	all	Specifies all switches in the VCS cluster.

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 If the RBridge ID is not provided, status results default to the local switch (LOCL). If **rbridge-id all** is specified, the command displays the status for all switches in the cluster.

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 overlapping-vlan-resource usage

Shows the utilization of the hardware table entries that support classified or transport VLAN classifications that use overlapping C-TAGs in a Virtual Fabrics context.

Synopsis **show overlapping-vlan-resource usage**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to see entries for classified or transport VLANs in a Virtual Fabrics context.

Usage Guidelines This command is platform-specific. For platforms that do not have such a table for classified or TLS VLANs, the percentage is zero.

Examples

```
switch# show overlapping-vlan-resource usage
Number of table entries used:6.11%(max 4028, used 246)
```

See Also None

show overlay-gateway

Displays status and statistics for the VXLAN overlay-gateway instance.

Synopsis	show overlay-gateway [name <i>name</i> [<i>vlan statistics</i>]] [<i>rbridge-id rbridge-id</i>] [<i>statistics</i>]				
Operands	<i>name</i>	Name of the configured VXLAN gateway. Network OS supports only one gateway instance.			
	vlan statistics	Displays statistics for each VLAN for the VXLAN gateway. Statistics include transmitted and received packet counts and byte counts exchanged for each exported VLAN. Because each exported VLAN maps to a VXLAN, these statistics apply on a per-VXLAN-counters basis. Per-VLAN counters are not enabled by default. You need to first run the enable statistics direction command for the gateway to enable statistics for specified VLAN IDs.			
	<i>rbridge-id</i>	Filters gateway status for a specific Rbridge ID.			
	statistics	Displays statistics for the VXLAN gateway. Statistics include transmitted and received packet counts and byte counts. These counters are derived by aggregating tunnel counters for all the tunnels of the gateway.			
Defaults	None				
Command Modes	Privileged EXEC mode				
Description	Displays status and statistics for the VXLAN overlay-gateway instance. Output includes the gateway name, the system-assigned gateway ID, source IP address, VRF, administration state, number of tunnels associated, and the Rbridge IDs on which the gateway is configured.				
Usage Guidelines	This command is available only for a switch that is in logical chassis cluster mode.				
	If you specify the gateway name, the gateway must already be configured.				
Examples	To show the status for the gateway instance:				
	<pre>sw0# show overlay-gateway Overlay Gateway "xx", ID 1, rbridge-ids 22-23 Admin state up IP address 100.1.1.110 (ve1000, Vrid 100), Vrf default-vrf Number of tunnels 2 Packet count: RX 0 TX 0 Byte count : RX (NA) TX 0</pre>				
	To show statistics for the gateway instance:				
	<pre>sw0# show overlay-gateway statistics Gateway Name RX packets TX packets RX bytes TX bytes ===== ===== GW1 200000 10000 22227772 1110111</pre>				

To display statistics for VLANs attached to the VXLAN gateway:

Example 1

```
sw0# show overlay-gateway name GW1 vlan statistics
```

VLAN	VNI	Tx	Rx	Packets	Bytes
				Tx	Rx
10	1010	10000	200000	1110111	22227772
11	1011	2200	-	221334	-
21	1021	-	1	-	100

Example 2

```
sw0# show overlay-gateway name test vlan statistics
```

VLAN ID	RX packets	TX packets
30	0	0
40	3696	3696

See Also

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**] [**details** *polycyname*]

Operands **interface tengigabitethernet** *rbridge-id/slot/port*

Interface where policy-map is bound.

input | **output** Direction (inbound or outbound) where the policy-map is applied.

details *polycyname* Displays the detail configuration of the policy-map along with binding information.

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 Enter **show policymap** for a specific interface to display the policy-map binding settings (policy-map name and traffic direction), police-priority-map applied, and class-map Policer parameters applied for that interface.

Enter **show policymap** without identifying an interface and direction of traffic to display policy-map binding for all interfaces on the switch.

NOTE

This command is only supported on Brocade VDX 8770-4, VDX 8770-8, and later switches.

The 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.

Examples To display policy-map binding and class-map parameters applied to a specific interface:


```
switch# show policymap interface tengigabitethernet 4/1 input
Interface : Ten Gigabit Ethernet 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 : Ten Gigabit Ethernet 4/2
Inbound policy map is policymapA-1
Outbound policy map is not set

Interface : Ten Gigabit Ethernet 4/3
Inbound policy map is not set
Outbound policy map is not set

Interface : Ten Gigabit Ethernet 4/4
Inbound policy map is not set
Outbound policy map is not set
```

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. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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 number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.

detail Displays detailed LAG information for a port-channel.

load-balance Displays the load-balance or frame-distribution scheme among ports in the port-channel.

summary Displays the summary information per channel-group.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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.

When using the **show port-channel** *channel-group-number* command, an asterisk in the command output designates that the designated port channel is the primary link through which the BUM (Broadcast, Unknown unicast and Multicast) traffic flows.

Examples To display detailed port-channel information:

```
switch# show port-channel detail
LACP Aggregator: Po 10 (vLAG) (Defaulted)
Aggregator type: Standard
Ignore-split is enabled
Member rbridges:
rbridge-id: 1 (2)
rbridge-id: 2 (1)
Actor System ID - 0x8000,01-e0-52-00-00-01
Admin Key: 0010 - Oper Key 0010
Receive link count: 1 - Transmit link count: 1
Individual: 0 - Ready: 1
Partner System ID - 0x8000,00-05-1e-cd-0f-ea
Partner Oper Key 0010
Member ports on rbridge-id 2:
Link: Te 2/0/7 (0x218038006) sync: 1
```

See Also None

show port-profile

Displays the AMPP port-profile configuration information.

Synopsis	show port-profile
Operands	None
Defaults	None
Command Modes	Privileged EXEC mode
Description	Use this command to display the port profile configuration information.
Usage Guidelines	None
Examples	Example of this command: <pre> 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 </pre>
See Also	show running-config, show port-profile interface, show port-profile

show port-profile domain

Displays the status of Automatic Migration of Port Profiles (AMPP) profiles and port-profile domains.

Synopsis **show port-profile** [*port-profile-name*] | **domain** *port-profile-domain-name*] [**status** | **activated** | **applied**] | **associated**]

Operands

<i>port-profile-name</i>	The name of a port-profile.
domain	Enables specification of a port-profile domain name.
<i>port-profile-domain-name</i>	Name of a port-profile domain.
status	Enables selection of status type.
activated	Specifies all port-profiles with the activated status.
applied	Specifies all port-profiles with the applied status.
associated	Specifies all port-profiles with the associated status.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the status of an AMPP port-profile or port-profile domain.

Usage Guidelines Enter **show port-profile status** to display the status of all AMPP profiles.
If no option is specified, then all port-profiles that match the criteria are shown.

Examples The following example shows the status of all port-profiles:

```
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
```

The following example shows the status of a port-profile domain:

```
switch# show port-profile domain vDC1_Domain status
Port-Profile      PPID      Activated      Associated MAC      Interface
Tenant1_PP        1         No             None                None
Tenant2_PP        2         No             None                None
```

See Also **show running-config**, **show running-config port-profile-domain**, **show port-profile**, **show port-profile interface**

show port-profile interface

Displays AMPP port-profile information for interfaces.

Synopsis **show port-profile interface** [**all** | **port-channel** *channel-group-number* | **fortygigabitethernet** *rbridge-id/slot/port* | **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. Valid values range from 1 through 63 for standalone mode, and 1 through 6144 for Brocade VCS Fabric mode.

fortygigabitethernet *rbridge-id/slot/port*
Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the 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 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 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	<i>port-profile-name</i>	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 Use this command to display the port-profile information for a named port-profile.

Usage Guidelines None

Examples None

See Also None

show port-security

Displays the configuration information related to port security.

Synopsis **show port-security**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the configuration information related to port security.

Usage Guidelines None

Examples

```
switch# show port-security
Secure  MaxSecureAddr  CurrentAddr  StaticSec  Violated Action  OUIs Sticky
Port      (count)          (count)      (count)
Te 1/1    2                  1            3          No       Restrict 2    No
Te 1/3    3                  3            5          Yes      Shutdown 0    Yes
```

See Also None

show port-security addresses

Displays the configuration information related to port-security addresses.

Synopsis **show port-security addresses**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the configuration information related to port-security addresses.

Usage Guidelines None

Examples switch# **show port-security addresses**

```

                                Secure Mac Address Table
-----
Vlan          Mac Address      Type           Ports
-----
1             0000.0000.0001    Secure-Dynamic 1/1
1             0000.0000.0002    Secure-Static  1/2
```

See Also None

show port-security interface

Displays the configuration information related to port-security interfaces.

Synopsis **show port-security interface** [**all** | **port-channel** *channel-group-number* | **fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands **all** Displays the port-security information for all interfaces.

port-channel *channel-group-number*
Specifies a LAG port channel-group number to display. Valid values range from 1 through 63 for standalone mode, and 1 through 6144 for Brocade VCS Fabric mode.

fortygigabitethernet *rbridge-id/slot/port*
Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the 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 configuration information related to port-security interfaces.

Usage Guidelines None

Examples

```
switch# show port-security interface TenGigabitEthernet 1/1
Port Security           :Enabled
Port Status             :up / Down (Security Violated)
Violation Mode          :Restrict
Violated                :Yes/No
Sticky enabled          :Yes/No
Maximum MAC Addresses   :2
Total MAC Addresses     :2
Configured MAC Addresses :5
```

```
Violation time      : Fri Mar 22 05:53:03 UTC 2013
Shutdown time(in Minutes) :5
Number of OUIs configured :1
```

See Also None

show port-security oui interface

Displays the configuration information related to port security for Organizationally Unique Identifier (OUI) interfaces.

Synopsis **show port-security oui interface**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the configuration information related to port-security for OUI interfaces.

Usage Guidelines None

Examples switch# **show port-security oui interface TenGigabitEthernet 1/1**
OUIs configured : 3
OUIs : 0010.0a00.0000
 0020.0b00.0000
 0030.0c00.0000

See Also None

show port-security sticky interface

Displays the configuration information related to port security for a sticky interface.

Synopsis **show port-security sticky interface**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the configuration information related to port-security for a sticky interface.

Usage Guidelines None

Examples switch# **show port-security sticky interface TenGigabitEthernet 1/1**

VlanId	Mac-address	Type	State	Ports
1	0000.0000.1111	Secure-Sticky	Active	Te 1/1

See Also None

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**] [**history**] [**top**]

Operands **rbridge-id** Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:

- rbridge-id* Specifies the RBridge ID. This parameter is not valid in standalone mode, and is supported only for the local RBridge ID.
- all** Specifies all switches in the fabric.
- summary** Displays a summary view of cpu usage.
- history** Displays the history of CPU usage.
- top** Displays current CPU utilization.

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 **rbridge-id** Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:

rbridge-id Specifies the RBridge ID. This parameter is supported only for the local RBridge ID.

all Specifies all switches in the fabric. This parameter 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 **More** in the terminal window 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 **rbridge-id** Executes the command on the specified switches. Valid completions for **rbridge-id** include the following:

- rbridge-id* Specifies the RBridge ID. This parameter is not valid in standalone mode, and is supported only for the local RBridge ID.
- all** Specifies all switches in the fabric. This parameter is not supported.
- summary** Displays a summary view of memory usage.

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 memory usage information by individual processes:

```
switch# show process memory
%Memory Used: 23.0904%; TotalMemory: 6191688 KB; Total Used: 1429688 KB
Total Free: 4762000 KB; Low Free: 868152 KB; High Free: 3034012 KB; Cached: 8067
24 KB
  PID  Process          MEM%      VSIZE (KB)      RSS (KB)      PSS (KB)
  ----  -
  2462  Dcmd.Linux.powe    2.10        251084        130764        104557
  2720  NosSmd.Linux.po    1.70        188892        109176         86360
  2799  postgres           1.20        185296         80080         63286
  3115  arpd               0.80        491404        49936         32129
  2362  raslogd            0.60        193396        41748         20436
  3099  nsm                0.60        189312        38064         20129
  3105  rtmd               0.60        247220        37600         19709
  2461  Ccmd.Linux.powe    0.50        140556        34192         17622
  1273  confd              0.50         37688        31288         30101
  3107  ssmd               0.50        238840        31128         13398
[output omitted, as will vary by device]
  13847  BLADE_INTR_7       0.00          0              0              0
  13848  BLADE_TMR_7        0.00          0              0              0
  13849  module-241-th      0.00          0              0              0
  13917  XMI_TX/207         0.00          0              0              0
  13918  XMI_RX/207         0.00          0              0              0
  13919  XMI_TX/247         0.00          0              0              0
  13920  XMI_RX/247         0.00          0              0              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 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** *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

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 the runtime state retrieved from the dataplane reflecting the operation of 802.3x pause or Priority Flow Control (PFC) on an interface.

Usage Guidelines 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* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display all of the configured flow control information for a 10-gigabit Ethernet interface:

```
switch# show qos flowcontrol interface tengigabitethernet 5/0/1
Interface Ten Gigabit Ethernet 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
  1  Off  Off  Off  Off
  2   On  Off   On  Off
  3  Off  Off  Off  Off
  4  Off  Off  Off  Off
                                0
                                0
                                0
                                0
                                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** *rbridge-id/slot/port*
Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
Specifies a valid 1-gigabit 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 parameter to specify the interface.

port-channel *number*
Specifies the port-channel of the interface. Valid values range from 1 through 63.

all Reports QoS configurations for all interfaces within the system.

Defaults If no interface is specified, QoS information for all interfaces is displayed.

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 The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display all of the configured QoS information for a 10-gigabit Ethernet interface:

```
switch# show qos interface tengigabitethernet 22/0/1
Interface Ten Gigabit Ethernet 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 Report shows 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 Brocade VDX 8770-4, VDX 8770-8, and later switches.

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 maps and their application on interfaces.

Usage Guidelines None

Examples To display information on defined QoS DSCP-Traffic-Class 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 <i>rbridge-id/slot/port</i> Specifies a valid 10-gigabit Ethernet interface.

<i>rbridge-id</i>	Specifies the RBridge ID.

<i>slot</i>	Specifies a valid slot number.

<i>port</i>	Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
Specifies a valid 1-gigabit Ethernet interface.

<i>rbridge-id</i>	Specifies the RBridge ID.

<i>slot</i>	Specifies a valid slot number.

<i>port</i>	Specifies a valid port number.

all	Reports QoS statistics for all Ethernet interfaces within the system.

Defaults None

Command Modes

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 standalone switch, all ASICs are considered as slot number zero (0).

The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display the queueing information for a 10-gigabit Ethernet interface:

```
switch# show qos queue interface tengigabitethernet 5/0/2
Interface Ten Gigabit Ethernet 5/0/2
```

CoS	RX Packets	RX Bytes	TC	TX Packets	TX 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 of 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** *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

all Reports QoS configurations for all 10-gigabit Ethernet interfaces within the system.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display a summary of the runtime ingress queue state information applied to a Layer 2 interface.

Usage Guidelines The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

This command is not supported on Brocade VDX 8770-4 and VDX 8770-8 platforms.

Examples To display the runtime ingress queue state information retrieved from the dataplane for a 10-gigabit Ethernet interface:

```
switch# show qos rcv-queue interface tengigabitethernet 22/0/2
Interface Ten Gigabit Ethernet 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 <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 The **gigabitethernet** *rbridge-id/slot/port* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

This command is not supported on Brocade VDX 8770-4 and VDX 8770-8 switches.

For a standalone switch, all ASICs are considered as slot number zero (0).

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 Brocade VDX 8770-4, VDX 8770-8, and later switches.
Examples	Using show qos red profiles to display information on defined QoS RED profiles:

NOTE

Notice that the first example shows output for the RED profile configured in the example for the **qos red profile** command.

```
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
```

Using **show qos interface *interface-name*** to examine the applied RED profiles for a specific interface:

```
switch# show qos interface te 1/2/2
```

```
Interface Ten Gigabit Ethernet 1/2/2
```

```
    Provisioning mode non-cee
```

```
    Default CoS 0
```

```
    Interface COS trust untrusted
```

```
    CoS-to-CoS Mutation map 'default'
```

2 show qos red profiles

```
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 Random Early Discard (RED) statistics for a specific interface.

Synopsis **show qos red statistics interface** *interface-name*

Operands *interface-name* Name of interface where a RED profile is 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. Notice 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 rbridge-id

Displays the RBridge ID of each node that is configured in a Virtual Cluster Switching (VCS) cluster.

Synopsis **show rbridge-id** [**swbd-number** *int* | **chassis** {**virtual-ip**}

Operands **swbd-number** Selects a switch type.
 int One or more integers (including a decimal) that identifies a switch type.
chassis virtual-ip Displays virtual IP addresses if configured

Defaults None

Command Modes Privileged EXEC configuration mode

Description Use this command to view the RBridge IDs of configured nodes in a VCS cluster, in addition to the switch type (SWBD) number and IPv4 and IPv6 virtual IP addresses.

Usage Guidelines None

Examples switch# **show rbridge-id**
RBRIDGE SWBD
ID NUMBER V4 V6

154 95 - -

See Also rbridge-id

show rbridge-running config

Displays configuration for an RBridge ID.

Synopsis **show rbridge-running-config rbridge-id** *rbridge-id*

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID whose configuration will be displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Displays the currently running configuration for the specified RBridge ID.

Usage Guidelines None

Examples The following example shows partial output for this command:

```
switch# show rbridge-running-config rbridge-id 1
diag post rbridge-id 1
  enable
  !
  dpod 1/0/1
    reserve
  !
  dpod 1/0/2
    reserve
  !
  dpod 1/0/3
    reserve
  !
  dpod 1/0/4
  !
  dpod 1/0/5
  !
  dpod 1/0/6
  !
  dpod 1/0/7
  !
  dpod 1/0/8
  !
  dpod 1/0/9
  !
  dpod 1/0/10
  !
  dpod 1/0/11
  !
  dpod 1/0/12
  !
  dpod 1/0/13
  !
  dpod 1/0/14
  !
  dpod 1/0/15
  !
  dpod 1/0/16
  !
```

2 show rbridge-running config

```
dpod 1/0/17
!
dpod 1/0/18
!
dpod 1/0/19
!
dpod 1/0/20
!
dpod 1/0/21
!
dpod 1/0/22
!
dpod 1/0/23
!
dpod 1/0/24
!
logging 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 VDX6720-24
  host-name rb1
!
no support autoupload enable
support 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 user snmpadmin1 groupname snmpadmin
snmp-server user snmpadmin2 groupname snmpadmin
snmp-server user snmpadmin3 groupname snmpadmin
snmp-server user snmpuser1
snmp-server user snmpuser2
snmp-server user snmpuser3
line vty
  exec-timeout 10
!
zoning enabled-configuration cfg-name ""
zoning enabled-configuration default-zone-access allaccess
zoning enabled-configuration cfg-action cfg-save
role name admin desc Administrator
role name user desc User
aaa authentication login local
aaa accounting exec default start-stop none
aaa accounting commands default start-stop none
service password-encryption
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
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-priority priority 0
!
fcoe
fabric-map default
vlan 1002
priority 3
virtual-fabric 128
fcmap 0E:FC:00
max-enodes 64
advertisement interval 8000
keep-alive timeout
!
map default
fabric-map default
cee-map default
!
!
interface Vlan 1
shutdown
!
interface Vlan 123
shutdown
!
fabric route mcast rbridge-id 1
!
protocol lldp
advertise dcbx-fcoe-app-tlv
advertise dcbx-fcoe-logical-link-tlv
advertise dcbx-tlv
system-description Brocade-VDX-VCS 300
!
vlan dot1q tag native
port-profile default
vlan-profile
switchport
switchport mode trunk
switchport trunk allowed vlan all
switchport trunk native-vlan 1
!
!
class-map cee
!
class-map default
!
rbridge-id 1
ip route 0.0.0.0/0 10.17.0.1
switch-attributes chassis-name VDX6720-24
switch-attributes host-name rb1
```

2 show rbridge-running config

```
system-monitor fan threshold marginal-threshold 1 down-threshold 2
system-monitor fan alert state removed action raslog
system-monitor power threshold marginal-threshold 1 down-threshold 2
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 2
system-monitor cid-card alert state none action none
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 2
system-monitor LineCard alert state none action none
system-monitor SFM threshold marginal-threshold 1 down-threshold 2
no protocol vrrp
no protocol vrrp-extended
interface Ve 123
    shutdown
!
!
interface Management 1/0
    no ip address dhcp
    ip address 10.17.10.21/20
    ip gateway-address 10.17.0.1
    no ipv6 address autoconfig
    no ipv6 address dhcp
!
interface TenGigabitEthernet 1/0/1
    description LC 1/0/1-23
    fabric isl enable
    fabric trunk enable
    no shutdown
!
interface TenGigabitEthernet 1/0/2
    description LC 1/0/1-23
    fabric isl enable
    fabric trunk enable
    no shutdown
!
interface TenGigabitEthernet 1/0/3
    mtu 9216
    description LC 1/0/1-23
    fabric isl enable
    fabric trunk enable
```

See Also **show global-running-config, show rbridge-local-running-config**

show rbridge-local-running-config

Displays local configuration for an RBridge ID.

Synopsis **show rbridge-local-running-config rbridge-id** *rbridge-id*

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID whose configuration will be displayed.

Defaults None

Command Modes Privileged EXEC mode

Description Displays the currently local running configuration for the specified RBridge ID.

Usage Guidelines None

Examples The following example shows partial output for this command:

```
switch# show rbridge-local-running-config rbridge-id 1
diag post rbridge-id 1
  enable
  !
  dpod 1/0/1
    reserve
  !
  dpod 1/0/2
    reserve
  !
  dpod 1/0/3
    reserve
  !
  dpod 1/0/4
  !
  dpod 1/0/5
  !
  dpod 1/0/6
  !
  dpod 1/0/7
  !
  dpod 1/0/8
  !
  dpod 1/0/9
  !
  dpod 1/0/10
  !
  dpod 1/0/11
  !
  dpod 1/0/12
  !
  dpod 1/0/13
  !
  dpod 1/0/14
  !
  dpod 1/0/15
  !
  dpod 1/0/16
  !
```

2 show rbridge-local-running-config

```
dpod 1/0/17
!
dpod 1/0/18
!
dpod 1/0/19
!
dpod 1/0/20
!
dpod 1/0/21
!
dpod 1/0/22
!
dpod 1/0/23
!
dpod 1/0/24
!
switch-attributes 1
  chassis-name VDX6720-24
  host-name rb1
!
fabric route mcast rbridge-id 1
!
rbridge-id 1
  ip route 0.0.0.0/0 10.17.0.1
  switch-attributes chassis-name VDX6720-24
  switch-attributes host-name rb1
  system-monitor fan threshold marginal-threshold 1 down-threshold 2
  system-monitor fan alert state removed action raslog
  system-monitor power threshold marginal-threshold 1 down-threshold 2
  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 2
  system-monitor cid-card alert state none action none
  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 2
  system-monitor LineCard alert state none action none
  system-monitor SFM threshold marginal-threshold 1 down-threshold 2
  no protocol vrrp
  no protocol vrrp-extended
  interface Ve 123
    shutdown
  !
!
interface Management 1/0
  no ip address dhcp
  ip address 10.17.10.21/20
  ip gateway-address 10.17.0.1
  no ipv6 address autoconfig
  no ipv6 address dhcp
!
interface TenGigabitEthernet 1/0/1
  description LC 1/0/1-23
  fabric isl enable
  fabric trunk enable
  no shutdown
!
interface TenGigabitEthernet 1/0/2
  description LC 1/0/1-23
```

```
fabric isl enable
fabric trunk enable
no shutdown
!
interface TenGigabitEthernet 1/0/3
mtu 9216
description LC 1/0/1-23
fabric isl enable
fabric trunk enable
switchport
switchport mode access
switchport access vlan 1
no shutdown
!
interface TenGigabitEthernet 1/0/4
mtu 9216
description LC 1/0/1-23
```

See Also **show global-running-config, show rbridge-running config**

show redundancy

Displays the control processor redundancy settings of the Management Module (MM).

Synopsis	show redundancy
Operands	None
Defaults	None
Command Modes	Privileged EXEC mode
Description	Use this command to display the redundancy settings of the MM.
Usage Guidelines	None
Examples	To show redundancy: <pre>switch# show redundancy === MM Redundancy Statistics === Current Active Session: Active Slot = M2 (Local), Failover Cause: Failed Over Standby Slot = M1 (Remote) Start Time: 11:11:08 UTC Wed Nov 28 2012 Previous Active Session: Active Slot = M1 Standby Slot = M2 End Time: 09:50:07 UTC Wed Nov 28 2012 System Uptime: 09:42:12 UTC Wed Nov 28 2012</pre>
See Also	ha failover, ha enable, ha failover, show ha

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.
	<i>number</i>	Specifies the alarm index identification number. Valid values range from 1 through 65535.
	brief	Specifies to display a brief summary of the output.
	events	Specifies to display the RMON events table.
	<i>number</i>	Specifies the event index identification number. Valid values range from 1 through 65535.
	brief	Specifies to display a brief summary of the output.
	logs	Specifies to display the RMON log table.
	<i>event_number</i>	Specifies the event log index identification number. Valid values range from 1 through 65535.
	statistics	Specifies to display the statistics identification number.
	<i>number</i>	Specifies the statistics identification number. Valid values range 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 : Ten Gigabit Ethernet 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)
```

2 show rmon

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 RMONhistory identification number. Valid values range from 1 through 65535.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display a synopsis of the statistics collected by the **rmon event** and **rmon alarm** commands.

Usage Guidelines Add the **statistics** parameter to display the detailed history.

Examples To display the RMON history:

```
switch# show rmon history
RMON history control entry 1
  interface: ifIndex.1745682445 Ten Gigabit Ethernet 0/13
  buckets requested: 20
  buckets granted: 20
  sampling interval: 10
  Owner: jsmith
```

See Also **rmon alarm, rmon event**

show route-map

Displays all interfaces in the system that currently have a route map applied.

Synopsis **show route-map** [*name*] [**rbridge-id** *rbridge-id* | **all**]
show route-map ve *vlan-id* [**rbridge-id** *rbridge-id* | **all**]

Operands	<i>name</i>	The name of the route-map.
	ve <i>vlan_id</i>	Specifies the interface Ve for the mentioned RBridge ID.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node. Values can be a range of nodes or individual nodes and are separated by a comma.
	all	Specifies all identifiers for a node. The command applies to all of the nodes. The command applies to all of the nodes.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the range of reserved VLAN values.

Usage Guidelines Output indicators are as follows:

- **Active/Partial/Inactive status:** Indicates the instantiation of the route-map configuration into the underlying hardware. Possible meanings for inactive may be no room in the TCAM for programming the ACL, or the exhaustion of next-hop entries within the hardware next-hop table.
- **Selected:** Indicates which of the configured next hops is currently being used by the policy. If the keyword selected is absent from the display, it indicates that none of the next hops in the list is being used and the packet is being routed by the standard routing mechanism.
- **Count:** Provides a summary of the number of times any of the match criteria within the specific ACL has been hit. If the ACL binding was unable to allocate a counter for the ACL (due to resource exhaustion), the count value will show "Counter not available." Otherwise, an actual counter value is displayed.

Examples

```
sw0# show route-map
Interface TenGigabitEthernet 3/3
  Ip Policy Route-map abc

Interface TenGigabitEthernet 3/4
  Ip Policy Route-map bar
```

Example of **show route-map** by application:

```
sw0# show route-map abc
Interface TenGigabitEthernet 3/3
  ip policy route-map abc permit 10 (Active)
    match ip address acl ACL_Vincent
    set ip precedence critical
    set ip next-hop 3.3.1.1 (selected)
    set ip next-hop 4.4.2.1
```

```
Policy routing matches: 100 packets; 500000 bytes

ip policy route-map abc permit 20 (Active)
  match ip address acl ACL_Vincent_2
  set ip precedence flash
  set ip next-hop 10.3.1.1
  set ip next-hop 10.4.2.1 (selected)
  set ip interface null0
  Policy routing matches: 0 packets; 0 bytes

sw0# show route-map xyz
Interface TenGigabitEthernet 3/4
  ip policy route-map xyz deny 10 (inactive)
    match ip address acl Vincent
    set ip precedence critical
    set ip vrf pulp_fiction next-hop 3.3.3.5 (selected)
    set ip next-hop 4.4.4.4
    Policy routing matches: Counter not available

sw0# show route-map abc rbridge-id all
Interface TenGigabitEthernet 204/3/3
  ip policy route-map abc permit 10 (Active)
    match ip address acl ACL_Vincent
    set ip next-hop 3.3.1.1 (selected)
    set ip next-hop 4.4.2.1
    Policy routing matches: 100 packets; 500000 bytes

Interface Ve 3 on rbridge-id 205
  ip policy route-map abc permit 20 (Active)
    match ip address acl ACL_Vincent_2
    set ip next-hop 10.3.1.1
    set ip next-hop 10.4.2.1 (selected)
    set ip interface null0
    Policy routing matches: 0 packets; 0 bytes
```

See Also **ip policy route-map**

show route-map interface

Displays the status of a route-map application on the specified interface.

Synopsis **show route-map interface** [**port-channel** *index* | **gigabitethernet** *slot/port* | **tengigabitethernet** *slot/port* | **fortygigabitethernet** *slot/port* | **ve** *vlan-id*]

show route-map interface ve *vlan-id* **rbridge-id** [*rbridge-id* | **all**]

Operands **port-channel** *index* Displays the status of the port-channel interface.

gigabitethernet *slot/port*
 Displays the configuration of all 1-gigabit Ethernet interfaces on the local switch.

tengigabitethernet *slot/port*
 Displays the configuration of all 10-gigabit Ethernet interfaces on the local switch.

fortygigabitethernet *slot/port*
 Displays the configuration of all 40-gigabit Ethernet interfaces on the local switch.

ve *vlan-id* Displays the status of a route-map application on the specified virtual Ethernet interface Ve for the mentioned rbridge-id.

rbridge-id Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id Specifies a unique identifier for a node. Values can be a range of nodes or individual nodes and are separated by a comma.

all Specifies all identifiers for a node. The command applies to all of the nodes.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the status of a route-map application on the specified interface.

Usage Guidelines You do not need to specify the route map name, as only a single route map can be applied to an interface.

Examples To display the status of a route map on a 10-gigabit Ethernet interface:

```
sw0# show route-map interface tengigabitethernet 3/3
Interface TenGigabitEthernet 3/3
  ip policy route-map foo permit 10 (Active)
    match ip address acl ACL_Vincent
    set ip next-hop 3.3.1.1 (selected)
    set ip next-hop 4.4.2.1
    Policy routing matches: 100 packets; 500000 bytes

  ip policy route-map foo permit 20 (Active)
    match ip address acl ACL_Vincent_2
    set ip next-hop 10.3.1.1
    set ip next-hop 10.4.2.1 (selected)
```

```
set ip interface null0
Policy routing matches: 0 packets; 0 bytes

sw0# show route-map interface Ve 3 rbridge-id all
Interface Ve 3 on rbridge-id 205
ip policy route-map foo permit 10 (Active)
  match ip address acl ACL_Vincent
  set ip precedence critical
  set ip next-hop 3.3.1.1 (selected)
  set ip next-hop 4.4.2.1
Policy routing matches: 100 packets; 500000 bytes

Interface Ve 3 on rbridge-id 206
ip policy route-map foo permit 20 (Active)
  match ip address acl ACL_Vincent_2
  set ip next-hop 10.3.1.1
  set ip next-hop 10.4.2.1 (selected)
  set ip interface null0
Policy routing matches: 0 packets; 0 bytes
```

See Also [ip policy route-map](#)

2 show running reserved-vlan

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. This is the configuration that is currently active on the local switch but which is not saved persistently.

Usage Guidelines This command is supported only on the local switch.
Enter **show running-config ?** to display the list of available configuration entries.

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

Displays the AAA server configuration.

Synopsis	show running-config aaa [accounting [commands exec] authentication [login]]	
Operands	accounting	Configures Login or Command accounting
	commands	Enable/Disable Command accounting
	exec	Enable/Disable Login accounting
	authentication	Configures preferred order of Authentication output modifiers
	login	Configures the order of sources for login (default = 'local')
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 display 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	
	switch# show running-config aaa authentication	
	aaa authentication login radius local	
	switch# show running-config aaa authentication	
	aaa authentication login ldap local-auth-fallback	
See Also	aaa authentication	

show running-config aaa accounting

Displays 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 display the configuration attributes of AAA accounting services.

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 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

Displays currently configured ACLs in the running configuration.

Synopsis **show running-config** {**ip** | **ipv6** | **mac**} **access-list** {**standard** | **extended**} [**access-list** *NAME*]

Operands **access-list** *NAME* Specifies a Level 2 or Level 3 ACL.
ip | **ipv6** | **mac** Displays the configured rules of either a Layer 2 or Layer 3 ACL.
standard | **extended** Specifies the ACL type.

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 Ten Gigabit Ethernet 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 ag

Displays the configured N_Port to VF_Port mappings, port grouping information, and other parameters for Access Gateway (AG) mode.

Synopsis	show running-config ag <i>rbridge-id</i>
Operands	<i>rbridge-id</i> Specific RBridge identifier for a switch.
Defaults	Displays AG configuration on local switch when RBridge ID not used.
Command Modes	Privileged EXEC mode
Description	Use this command to display parameters configured for AG mode. This shows the factory-default configuration, unless parameters have been modified by the user.
Usage Guidelines	Consider the following when using LB mode with show running-config ag and show ag commands: • The only Port Grouping mode that you can enable or disable is lb mode. • When lb mode is disabled in a port group, the show running-config ag, show ag map, and show ag commands display the <i>configured</i> VF_Port to N_Port mapping. This is because configured and active mapping are the same. • When lb mode is enabled in a port group, show ag and show ag map commands display the active mapping only because VF_Port to N_Port mapping is based on the current distributed load across all N_Ports. The show running-config ag command displays the configured mapping only.

Examples The following example displays the running AG configuration for RBridge ID 1.

```
sw0# show running-config rbridge-id 1 ag
```

```

nport 1/0/1
  map fport interface Fcoe 1/1/1 1/1/9 1/1/17 1/1/25 1/1/33 1/1/41 1/1/49 1/1/57
!
nport 1/0/2
  map fport interface Fcoe 1/1/2 1/1/10 1/1/18 1/1/26 1/1/34 1/1/42 1/1/50 1/1/58
!
nport 1/0/3
  map fport interface Fcoe 1/1/3 1/1/11 1/1/19 1/1/27 1/1/35 1/1/43 1/1/51 1/1/59
!
nport 1/0/4
  map fport interface Fcoe 1/1/4 1/1/12 1/1/20 1/1/28 1/1/36 1/1/44 1/1/52 1/1/60
!
nport 1/0/5
  map fport interface Fcoe 1/1/5 1/1/13 1/1/21 1/1/29 1/1/37 1/1/45 1/1/53 1/1/61
!
nport 1/0/6
  map fport interface Fcoe 1/1/6 1/1/14 1/1/22 1/1/30 1/1/38 1/1/46 1/1/54 1/1/62
!
nport 1/0/7
  map fport interface Fcoe 1/1/7 1/1/15 1/1/23 1/1/31 1/1/39 1/1/47 1/1/55 1/1/63
!
nport 1/0/8
  map fport interface Fcoe 1/1/8 1/1/16 1/1/24 1/1/32 1/1/40 1/1/48 1/1/56 1/1/64
!
pg 0
  nport interface FibreChannel 1/0/1 1/0/2 1/0/3 1/0/4 1/0/5 1/0/6 1/0/7 1/0/8

```

2 show running-config ag

```

    modes lb
    rename pg0
!
timeout fnm 120
counter reliability 25
!
!
sw0# show running-config ag
ag
mapset nport 1/0/1 fports 1/1/1 1/1/92 1/1/173
mapset nport 1/0/2 fports 1/1/24 1/1/105 1/1/186
mapset nport 1/0/3 fports 1/1/37 1/1/118 1/1/199
mapset nport 1/0/4 fports 1/1/410 1/1/1211 1/1/2012
mapset nport 1/0/5 fports 1/1/513 1/1/1314 1/1/2115
mapset nport 1/0/6 fports 1/1/616 1/1/1417 1/1/2218
mapset nport 1/0/7 fports 1/1/719 1/1/1520 1/1/2321
mapset nport 1/0/8 fports 1/1/822 1/1/1623 1/1/24
staticmapadd nport 1/0/1 staticfports
    staticmapadd nport 1/0/2 staticfports
    staticmapadd nport 1/0/3 staticfports
.....
failback 1/0/5 true
failback 1/0/6 true
failback 1/0/7 true
vcs:
fabric-map default
    vlan 1002
    priority 3
    virtual-fabric 128
    fcmmap 0E:FC:00
```

See Also **show ag, show ag map**

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-config 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.
<i>pgid</i>	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-config 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-priority priority 0
!
```

See Also **priority-group-table**, **remap fabric-priority**, **remap lossless-priority**

show running-config class-map

Displays configured class-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 Brocade VDX 8770-4, VDX 8770-8, and later switches.

Examples To display configured class maps:.

```
switch# show running-config class-map  
class-map default  
    match any
```

See Also **qos cos**

2 show running-config diag post

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
```

See Also **diag post enable**

show running-config dot1x

Displays the IEEE 802.1x Port Authentication configuration.

Synopsis **show running-config dot1x [enable | test timeout]**

Operands	enable	Shows the configured state of globally enabled IEEE 802.1x port authentication.
	test timeout	Shows the configured timeout value in seconds for the IEEE 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 Dynamic Ports on Demand (DPOD) license information.

Synopsis **show running-config dpod** [*rbridge-id/slot/port*]

Operands

<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies the slot number.
<i>port</i>	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 Brocade VDX 6710 and VDX 8770 switches. These switches do not support the Dynamic Ports on Demand feature.

In 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 the RBridge ID.
priority 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 These examples display 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**

2 show running-config fcoe

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 Use this command to display 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

  priority 3
  virtual-fabric 128
  fcmap 0E:FC:00
  max-enodes 64
  enodes-config local
  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 E_Port-to-EX_Port authentication protocol parameters.

Synopsis **show running-config** [**rbridge-id** {*rbridge-id* | **all**}] **fcsp auth**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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 To display the protocol and policy:

Standalone mode

```
switch# show running-config fcsp auth
fcsp auth group 2
fcsp auth hash md5
fcsp auth policy switch off
```

In VCS mode

To display both protocol and policy (auth-type = all, group = 2, hash = md5, and switch policy = off)

```
swe52# show running-config rbridge-id 2 fcsp auth
rbridge-id 2
fcspauth auth-type all
fcspauth group 2
fcspauth hash sha1
fcspauth policy switch active
```

See Also **fcsp auth**, **fcsp auth-secret dhchap**, **show fcsp auth-secret dh-chap**

show running-config hardware connector

Displays the SFP configurations in the running-config.

Synopsis **show running-config hardware connector**

Operands None

Defaults Displays information for the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the SFP configuration for the specified switches.

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

Examples To display the SFP configuration on the local switch:

```
switch# show running-config hardware connector
hardware
connector 0/1
no sfp breakout
!
connector 0/2
sfp breakout
```

See Also clear support, copy support, show support, sfp breakout

show running-config interface fcoe

Displays the status of FCoE interfaces.

Synopsis **show running-config interface fcoe** [*vn-number/rbridge-id/front-port-number*]

Operands *vn-number/rbridge-id/front-port-number* Specifies a valid FCoE port interface.

vn-number Specifies the VN number for FCoE.

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

front-port-number Specifies the front 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	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 Gbps Fibre Channel ports: <code>idle-idle</code> , <code>arbff-arbff</code> , <code>idle-arbff</code> , or <code>aa-then-ia</code> .
	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: IO —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: <code>auto</code> , <code>1 Gbps</code> , <code>2 Gbps</code> , <code>4 Gbps</code> , or <code>8 Gbps</code> .
	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.

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.

Enter **interface FibreChannel** to set the values.

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 fortygigabitethernet

Displays the status of 40-gigabit Ethernet interfaces.

Synopsis **show running-config interface fortygigabitethernet** [*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 Displays the configuration of all 40-gigabit Ethernet interfaces on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the configuration of 40-gigabit Ethernet interfaces.

Usage Guidelines None

Examples To display configuration information about all 40-gigabit Ethernet interfaces on a Brocade VDX 6710 switch:

```
switch# show running-config interface fortygigabitethernet
  interface Forty Gigabit Ethernet 22/0/49
    fabric isl enable
    fabric trunk enable
    no shutdown
    !
  interface Forty Gigabit Ethernet 22/0/50
    fabric isl enable
    fabric trunk enable
    no shutdown
    !
  interface Forty Gigabit Ethernet 22/0/51
    fabric isl enable
    fabric trunk enable
    no shutdown
    !
  interface Forty Gigabit Ethernet 22/0/52
    fabric isl enable
    fabric trunk enable
    sflow enable
    no shutdown
    !
  interface Forty Gigabit Ethernet 22/0/53
    fabric isl enable
    fabric trunk enable
    sflow enable
    shutdown
    !
  interface Forty Gigabit Ethernet 22/0/54
    fabric isl enable
    fabric trunk enable
```

See Also **interface**

show running-config interface fortygigabitethernet bpdudrop

Displays the BPDU drop status of a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **bpdudrop** [**enable**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	enable	Displays the drop status of STP/MSTP/RSTP and PVST+/R-PVST+ BPDUs.

Defaults None

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 v4.1.0 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 40-gigabit Ethernet port:

```
switch# show running-config interface fortygigabitethernet 1/0/49 bpdudrop
```

See Also **interface**

2 show running-config interface fortygigabitethernet cee

show running-config interface fortygigabitethernet cee

Displays whether the default CEE map has been applied to a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*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 None

Command Modes Privileged EXEC mode

Description Use this command to determine whether the default CEE map has been applied to a 40-gigabit Ethernet interface.

Usage Guidelines This command does not apply to ISL ports.

Examples None

See Also **cee**

show running-config interface fortygigabitethernet channel-group

Displays channel group configuration information for a 40-gigabit Ethernet interface participating in link aggregation.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **channel-group** [*mode | type*]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 standards-based LAG, or Brocade proprietary hardware-based trunking).

Defaults None

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 fortygigabitethernet description

Displays the description string associated with a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*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 None

Command Modes Privileged EXEC mode

Description Use this command to display the description string associated with the specified interface.

Usage Guidelines None

Examples switch# **show running-config interface fortygigabitethernet 1/0/52 description**
 interface fortygigabitethernet 1/0/52
 description Connects to storage device 1

See Also **description (interfaces), interface**

show running-config interface fortygigabitethernet dot1x

Displays IEEE 802.1x port-based access control configuration information for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **dot1x** [**authentication** | **port-control** | **protocol-version** | **quiet-period** | **reauthMax** | **reauthentication** | **timeout** | **re-authperiod** | **server-timeout** | **supp-timeout** | **tx-period**]]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 None

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 None

Examples To display the 802.1x port-based authentication configuration for a 40-gigabit Ethernet interface:

```
switch# show running-config interface fortygigabitethernet 1/0/49 dot1x
interface fortygigabitethernet 1/0/49
dot1x authentication
dot1x port-control auto
dot1x quiet-period 120
```

2 show running-config interface fortygigabitethernet dot1x

```
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 fortygigabitethernet fabric

Displays fabric protocol configuration parameters for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **fabric** [**isl** [**enable**] | **trunk** [**enable**]]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	isl [enable]	Indicates only the administration and operational state the Inter-Switch Link (ISL).
	trunk [enable]	Indicates only whether trunking is enabled on the port.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display ISL and trunking status for the specified interface.

Usage Guidelines None

Examples switch# **show running-config interface fortygigabitethernet 1/0/49 fabric**
 interface fortygigabitethernet 1/0/49
 fabric isl enable
 fabric trunk enable

See Also fabric isl enable, fabric trunk enable

2 show running-config interface fortygigabitethernet fcoeport

show running-config interface fortygigabitethernet fcoeport

Displays whether a 40-gigabit Ethernet interface is configured as an FCoE port.

Synopsis **show running-config interface fortygigabitethernet** [*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 None

Command Modes Privileged EXEC mode

Description Use this command to determine whether a 40-gigabit Ethernet port is configured for FCoE.

Usage Guidelines None

Examples None

See Also **fcoe, fcoeport**

show running-config interface fortygigabitethernet lacp

Displays interface configuration parameters for the Link Aggregation Control Protocol (LACP) for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **lacp** [**timeout**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	timeout	Indicates whether the interface timeout is short (for Brocade trunks) or long (for standard trunks).

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display LACP settings for the specified interface.

Usage Guidelines None

Examples None

See Also **lacp timeout**

show running-config interface fortygigabitethernet lldp

Displays Link Layer Discovery Protocol (LLDP) configuration information for a 40-gigabit Ethernet interface.

Synopsis	show running-config interface fortygigabitethernet [<i>rbridge-id/slot/port</i>] lldp [dcbx-version disable iscsi-priority profile]	
Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to display Link Layer Discovery Protocol (LLDP) configuration information for the specified interface.	
Usage Guidelines	None	
Examples	None	
See Also	lldp dcbx-version, lldp disable, lldp iscsi-priority, lldp profile	

show running-config interface fortygigabitethernet mac

Displays configured MAC parameters for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **mac** [**access-group**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	access-group	Displays MAC ACLs configured for the specified interface.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configured MAC parameters for the specified 40-gigabit Ethernet interface.

Usage Guidelines None

Examples None

See Also **mac access-group**

2 show running-config interface fortygigabitethernet mtu

show running-config interface fortygigabitethernet mtu

Displays the configured MTU for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*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 None

Command Modes Privileged EXEC mode

Description Use this command to display the configured MTU for the specified interface.

Usage Guidelines None

Examples switch# **show running-config interface fortygigabitethernet 1/0/49 mtu**
 interface fortygigabitethernet 1/0/49
 mtu 2500

See Also ip mtu

show running-config interface fortygigabitethernet port-profile-port

Displays whether AMPP port-profile configuration mode is enabled for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*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 None

Command Modes Privileged EXEC mode

Description Use this command to display whether AMPP port-profiling is configured for the specified interface.

Usage Guidelines None

Examples switch# **show running-config interface fortygigabitethernet 1/0/50**
 port-profile-port
 interface fortygigabitethernet 1/0/50
 port-profile-port

See Also **port-profile-port**

show running-config interface

fortygigabitethernet priority-tag

Displays whether 802.1p priority tagging is configured for a 40-gigabit Ethernet interface.

Synopsis	show running-config interface fortygigabitethernet [<i>rbridge-id/slot/port</i>] priority-tag	
Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to display whether 802.1p priority tagging is configured for the specified interface.	
Usage Guidelines	None	
Examples	<pre>switch# show running-config interface fortygigabitethernet 1/0/51 priority-tag interface fortygigabitethernet 1/0/51 priority-tag</pre>	
See Also	priority-tag	

show running-config interface fortygigabitethernet qos

Displays the Quality of Service (QoS) configuration for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **qos** [**cos** | **cos-mutation** | **cos-traffic-class** | **flowcontrol** [**rx** | **tx**] | **trust** [**cos**]]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	cos	Displays only the Class of Service (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 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 None

Examples None

See Also **qos cos**, **qos cos-mutation**, **qos cos-traffic-class**, **qos flowcontrol tx rx**, **qos trust cos**, **show qos flowcontrol interface**, **show qos interface**, **show qos queue interface**, **show qos rcv-queue interface**

show running-config interface fortygigabitethernet rmon

Displays the Remote Monitoring protocol (RMON) configuration for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **rmon** [**collection** [**history** *index* | **stats** *index*]]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	collection	Displays configuration information for RMON collections.
	history	Displays configuration information for RMON history collections.
	<i>index</i>	Specifies a valid RMON history collection index value.
	stats	Displays configuration information for RMON statistics collections.
	<i>index</i>	Specifies a valid RMON collection control index value.

Defaults 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 None

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/49 rmon collection
interface fortygigabitethernet 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 fortygigabitethernet sflow

Displays the sFlow configuration for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **sflow** [**enable** | **polling-interval** | **sample-rate**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 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 None

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/53 sflow
interface fortygigabitethernet 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 fortygigabitethernet shutdown

Displays whether a 40-gigabit Ethernet interface is enabled.

Synopsis **show running-config interface fortygigabitethernet** [*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 None

Command Modes Privileged EXEC mode

Description Use this command to display whether the specified 40-gigabit Ethernet interface is enabled.

Usage Guidelines None

Examples switch# **show running-config interface fortygigabitethernet 1/0/52 shutdown**
 interface fortygigabitethernet 1/0/52
 no shutdown

See Also **shutdown**

show running-config interface fortygigabitethernet switchport

Displays the configured switching characteristics for the 40-gigabit Ethernet Layer 2 interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id* | *slot* | *port*] **switchport** [*access* [*vlan*] | *mode* | *trunk* [*allowed* [*vlan*] | *native-vlan* | *tag* [*native-vlan*]]]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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	Displays native VLAN tags.

Defaults 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 None

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/49 switchport
interface fortygigabitethernet 1/0/49
switchport
switchport mode access
switchport access vlan 1
```

See Also switchport, switchport access, switchport mode, switchport trunk allowed vlan rspan-vlan

show running-config interface fortygigabitethernet udd

Displays Unidirectional Link Detection Protocol (UDLD) configuration information for a 40-gigabit Ethernet interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*] **udd enable**

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	enable	Indicates whether UDLD is enabled on the interface.

Defaults This command has no defaults.

Command Modes Privileged EXEC mode

Description Use this command to display Unidirectional Link Detection Protocol (UDLD) configuration information for the specified interface.

Usage Guidelines None

Examples None

See Also None

show running-config interface fortygigabitethernet vlan

Displays information about VLAN classification groups for a 40-gigabit Ethernet Layer 2 interface.

Synopsis **show running-config interface fortygigabitethernet** [*rbridge-id/slot/port*]
vlan [**classifier** [**activate** [**group**]]]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 None

Command Modes Privileged EXEC mode

Description Use this command to display VLAN classifier commands executed for the port.

Usage Guidelines None

Examples

```
switch# show running-config interface fortygigabitethernet 1/0/49 vlan
interface fortygigabitethernet 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 gigabitethernet

Displays the status of 1-gigabit 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 Displays the configuration of all 1-gigabit Ethernet interfaces on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the configuration of 1-gigabit Ethernet interfaces.

Usage Guidelines This command can be used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display configuration information about all 1-gigabit Ethernet interfaces on the local switch:

```
switch# show running-config interface gigabitethernet
interface Gigabit Ethernet 22/0/1
  description tests
  channel-group 2 mode active type standard
  lacp timeout long
  sflow enable
  no shutdown
!
interface Gigabit Ethernet 22/0/2
  channel-group 2 mode active type standard
  lacp timeout long
  no shutdown
!
interface Gigabit Ethernet 22/0/3
  channel-group 2 mode active type standard
  lacp timeout long
  no shutdown
!
interface Gigabit Ethernet 22/0/4
  no shutdown
!
interface Gigabit Ethernet 22/0/5
  no shutdown
!
interface Gigabit Ethernet 22/0/6
  no shutdown
!
interface Gigabit Ethernet 22/0/7
  no shutdown
(output truncated)
```

See Also **interface**

show running-config interface gigabitethernet bpdudrop

Displays the BPDUDrop status of a 1-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **bpdudrop** [**enable**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	enable	Displays the drop status of STP/MSTP/RSTP and PVST+/R-PVST+ BPDUs.

Defaults None

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 Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Brocade Network OS v4.1.0 supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples To display BPDUDrop status information for a specific 1-gigabit Ethernet port:

```
switch# show running-config interface gigabitethernet 1/0/7 bpdudrop
```

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	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 standards-based LAG, or Brocade proprietary hardware-based trunking).

Defaults None

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 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-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **description**

Operands

<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.

Defaults None

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 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 Gigabit Ethernet 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-gigabit 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	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 None

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 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-gigabit Ethernet interface:

```
switch# show running-config interface gigabitethernet 1/0/7 dot1x
interface Gigabit Ethernet 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-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **lacp** [**timeout**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	timeout	Indicates whether the interface timeout is short (for Brocade trunks) or long (for standard trunks).

Defaults None

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 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-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **lldp** [**dcbx-version** | **disable** | **iscsi-priority** | **profile**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 None

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 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-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **mac** [**access-group**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	access-group	Displays MAC ACLs configured for the specified interface.

Defaults None

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 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-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **mtu**

Operands

<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.

Defaults None

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 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 Gigabit Ethernet 1/0/8
  mtu 2500
!
```

See Also **ip mtu**

2 show running-config interface gigabitethernet port-profile-port

show running-config interface gigabitethernet port-profile-port

Displays whether AMPP port-profile configuration mode is enabled for a 1-gigabit 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 None

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 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 Gigabit Ethernet 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-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **priority-tag**

Operands

<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.

Defaults None

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 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 Gigabit Ethernet 1/0/8
priority-tag
```

See Also **priority-tag**

show running-config interface gigabitethernet qos

Displays the Quality of Service (QoS) configuration for a 1-gigabit 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	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	cos	Displays only the Class of Service (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 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 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 rx**, **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-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **rmon** [**collection** [*history index* | *stats index*]]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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.
	<i>index</i>	Specifies a valid RMON collection control index value.

Defaults 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 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 Gigabit Ethernet 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-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **sflow** [**enable** | **polling-interval** | **sample-rate**]

Operands

<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	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 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 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 Gigabit Ethernet 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-gigabit Ethernet interface is enabled.

Synopsis `show running-config interface gigabitethernet [rbridge-id/slot/port] shutdown`

Operands

<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display whether the specified 1-gigabit Ethernet interface is enabled.

Usage Guidelines This command can be used only on 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 Gigabit Ethernet 1/0/8
no shutdown
```

See Also `shutdown`

show running-config interface gigabitethernet switchport

Displays the configured switching characteristics for the 1-gigabit 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	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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	Displays tags for the native VLAN.

Defaults 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 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 Gigabit Ethernet 1/0/8
switchport
switchport mode access
switchport access vlan 1
```

See Also `switchport`, `switchport access`, `switchport mode`, `switchport trunk allowed vlan rspan-vlan`

show running-config interface gigabitethernet udd

Displays Unidirectional Link Detection Protocol (UDLD) configuration information for a 1-gigabit Ethernet interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*] **udd enable**

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	enable	Indicates whether UDLD is enabled on the interface.

Defaults This command has no defaults.

Command Modes Privileged EXEC mode

Description Use this command to display Unidirectional Link Detection Protocol (UDLD) configuration information for the specified interface.

Usage Guidelines None

Examples None

See Also None

show running-config interface gigabitethernet vlan

Displays information about VLAN classification groups for the 1-gigabit Ethernet Layer 2 interface.

Synopsis **show running-config interface gigabitethernet** [*rbridge-id/slot/port*]
vlan [**classifier** [**activate** [**group**]]]

Operands

<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	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 None

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 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 Gigabit Ethernet 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.

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 **access-group** 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 This example displays 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 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-gigabit Ethernet interfaces.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*]

Operands

<i>rbridge-id</i>	Specifies a switch by the its RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.

Defaults Displays the configuration of all 10-gigabitEthernet interfaces on the local switch.

Command Modes Privileged EXEC mode

Description Use this command to display the configuration of 10-gigabit Ethernet interfaces.

Usage Guidelines None

Examples To display configuration information about all 10-gigabit Ethernet interfaces on a Brocade VDX 6710 switch:

```
switch# show running-config interface tengigabitethernet
  interface Ten Gigabit Ethernet 22/0/49
    fabric isl enable
    fabric trunk enable
    no shutdown
  !
  interface Ten Gigabit Ethernet 22/0/50
    fabric isl enable
    fabric trunk enable
    no shutdown
  !
  interface Ten Gigabit Ethernet 22/0/51
    fabric isl enable
    fabric trunk enable
    no shutdown
  !
  interface Ten Gigabit Ethernet 22/0/52
    fabric isl enable
    fabric trunk enable
    sflow enable
    no shutdown
  !
  interface Ten Gigabit Ethernet 22/0/53
    fabric isl enable
    fabric trunk enable
    sflow enable
    shutdown
  !
  interface Ten Gigabit Ethernet 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-gigabit Ethernet interface.

Synopsis	show running-config interface tengigabitethernet [<i>rbridge-id/slot/port</i>] bpdu-drop [enable]	
Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	enable	Displays the drop status of STP/MSTP/RSTP and PVST+/R-PVST+ BPDUs.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to display information about dropped BPDUs on the specified 10-gigabit Ethernet interface.	
Usage Guidelines	STP, RSTP, or MSTP must be configured.	
	Brocade Network OS v4.1.0 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 10-gigabit Ethernet port:	
	switch# show running-config interface tengigabitethernet 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-gigabit Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*] **cee**

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to determine whether the default CEE map has been applied to a 10-gigabit Ethernet 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 a 10-gigabit Ethernet interface participating in link aggregation.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*] **channel-group** [**mode** | **type**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 standards-based LAG, or Brocade proprietary hardware-based trunking).

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about the channel group configuration of the specified 10-gigabit 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-gigabit 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 None

Command Modes Privileged EXEC mode

Description Use this command to display the description string associated with the specified 10-gigabit Ethernet interface.

Usage Guidelines None

Examples switch# **show running-config interface tengigabitethernet 1/0/52 description**
 interface tengigabitethernet 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-gigabit 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	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 None

Command Modes Privileged EXEC mode

Description Use this command to display configuration information for a 10-gigabit Ethernet interface configured for IEEE 802.1x port-based access control.

Usage Guidelines None

Examples To display the 802.1x port-based authentication configuration for a 10-gigabit Ethernet interface:

```
switch# show running-config interface tengigabitethernet 1/0/49 dot1x
interface tengigabitethernet 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-gigabit Ethernet interface.

Synopsis	show running-config interface tengigabitethernet [<i>rbridge-id/slot/port</i>] fabric [isl [enable] trunk [enable]]	
Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	isl [enable]	Indicates only the administration and operational state of the Inter-Switch Link (ISL).
	trunk [enable]	Indicates only whether trunking is enabled on the port.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to display ISL and trunking status for the specified 10-gigabit Ethernet interface.	
Usage Guidelines	None	
Examples	<pre>switch# show running-config interface tengigabitethernet 1/0/49 fabric interface tengigabitethernet 1/0/49 fabric isl enable fabric trunk enable</pre>	
See Also	fabric isl enable, fabric trunk enable	

show running-config interface tengigabitethernet fcoeport

Displays whether a 10-gigabit 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 None

Command Modes Privileged EXEC mode

Description Use this command to determine whether a 10-gigabit Ethernet port is configured for FCoE.

Usage Guidelines None

Examples None

See Also **fcoe, fcoeport**

2 show running-config interface tengigabitethernet lacp

show running-config interface tengigabitethernet lacp

Displays interface configuration parameters for the Link Aggregation Control Protocol (LACP) for a 10-gigabit Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*] **lacp** [**timeout**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	timeout	Indicates whether the interface timeout is short (for Brocade trunks) or long (for standard trunks).

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display LACP settings for the specified 10-gigabit Ethernet interface.

Usage Guidelines None

Examples None

See Also **lacp timeout**

show running-config interface tengigabitethernet lldp

Displays Link Layer Discovery Protocol (LLDP) configuration information for a 10-gigabit Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*] **lldp** [**dcbx-version** | **disable** | **iscsi-priority** | **profile**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 None

Command Modes Privileged EXEC mode

Description Use this command to display Link Layer Discovery Protocol (LLDP) configuration information for the specified 10-gigabit Ethernet interface.

Usage Guidelines None

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-gigabit Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*] **mac** [**access-group**]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	access-group	Displays MAC ACLs configured for the specified interface.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configured MAC parameters for the specified 10-gigabit Ethernet interface.

Usage Guidelines None

Examples None

See Also **mac access-group**

show running-config interface tengigabitethernet mtu

Displays the configured MTU for a 10 gigabit 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 None

Command Modes Privileged EXEC mode

Description Use this command to display the configured MTU for the specified 10-gigabit Ethernet interface.

Usage Guidelines None

Examples switch# **show running-config interface tengigabitethernet 1/0/49 mtu**
 interface tengigabitethernet 1/0/49
 mtu 2500

See Also ip mtu

2 show running-config interface tengigabitethernet port-profile-port

show running-config interface
tengigabitethernet port-profile-port

Displays whether AMPP port-profile configuration mode is enabled for a 10-gigabit Ethernet interface.

Synopsis	show running-config interface tengigabitethernet [<i>rbridge-id/slot/port</i>] port-profile-port	
Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to display whether AMPP port-profiling is configured for the specified 10-gigabit Ethernet interface.	
Usage Guidelines	None	
Examples	switch# show running-config interface tengigabitethernet 1/0/50 port-profile-port interface tengigabitethernet 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-gigabit Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*] **priority-tag**

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display whether 802.1p priority tagging is configured for the specified 10-gigabit Ethernet interface.

Usage Guidelines None

Examples switch# **show running-config interface tengigabitethernet 1/0/51 priority-tag**
interface tengigabitethernet 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-gigabit 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	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	cos	Displays only the Class of Service (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 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 10-gigabit Ethernet interface.

Usage Guidelines None

Examples None

See Also **qos cos**, **qos cos-mutation**, **qos cos-traffic-class**, **qos flowcontrol tx rx**, **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-gigabit Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*] **rmon** [**collection** [**history** *index* | **stats** *index*]]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	collection	Displays configuration information for RMON collections.
	history	Displays configuration information for RMON history collections.
	<i>index</i>	Specifies a valid RMON history collection index value.
	stats	Displays configuration information for RMON statistics collections.
	<i>index</i>	Specifies a valid RMON collection control index value.

Defaults Displays all RMON collection configuration information.

Command Modes Privileged EXEC mode

Description Use this command to display the RMON configuration for the specified 10-gigabit Ethernet interface.

Usage Guidelines None

Examples

```
switch# show running-config interface tengigabitethernet 1/0/49 rmon collection
interface tengigabitethernet 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-gigabit Ethernet interface.

Synopsis	show running-config interface tengigabitethernet [<i>rbridge-id/slot/port</i>] sflow [enable polling-interval sample-rate]	
Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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	Displays all sFlow configuration information for the port.	
Command Modes	Privileged EXEC mode	
Description	Use this command to display the sFlow configuration for the specified10-gigabit Ethernet interface.	
Usage Guidelines	None	
Examples	<pre>switch# show running-config interface tengigabitethernet 1/0/53 sflow interface tengigabitethernet 1/0/53 sflow enable sflow polling-interval 10 sflow sample-rate 100</pre>	
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-gigabit Ethernet interface is enabled.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*] **shutdown**

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display whether the specified 10-gigabit Ethernet interface is enabled.

Usage Guidelines None

Examples switch# **show running-config interface tengigabitethernet 1/0/52 shutdown**
 interface tengigabitethernet 1/0/52
 no shutdown

See Also shutdown

show running-config interface tengigabitethernet switchport

Displays the configured switching characteristics for the 10-gigabit 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	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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	Displays tags for the native VLAN.

Defaults 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 None

Examples

```
switch# show running-config interface tengigabitethernet 1/0/49 switchport
interface tengigabitethernet 1/0/49
switchport
switchport mode access
switchport access vlan 1
```

See Also switchport, switchport access, switchport mode, switchport trunk allowed vlan rspan-vlan

show running-config interface tengigabitethernet udd

Displays Unidirectional Link Detection Protocol (UDLD) configuration information for a 10 Gigabit Ethernet interface.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*] **udd enable**

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	enable	Indicates whether UDLD is enabled on the interface.

Defaults This command has no defaults.

Command Modes Privileged EXEC mode

Description Use this command to display Unidirectional Link Detection Protocol (UDLD) configuration information for the specified interface.

Usage Guidelines None

Examples None

See Also None

show running-config interface tengigabitethernet vlan

Displays information about VLAN classification groups for a 10-gigabit Ethernet Layer 2 interface.

Synopsis **show running-config interface tengigabitethernet** [*rbridge-id/slot/port*]
vlan [**classifier** [**activate** [**group**]]]

Operands	<i>rbridge-id</i>	Specifies a switch by its RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	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 None

Command Modes Privileged EXEC mode

Description Use this command to display VLAN classifier commands executed for the specified port.

Usage Guidelines None

Examples `switch# show running-config interface tengigabitethernet 1/0/49 vlan`
 `interface tengigabitethernet 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	<i>vlan_id</i>	Specifies a VLAN. Refer to the Usage Guidelines.
	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 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 On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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	<i>vlan_id</i>	Specifies a VLAN. Refer to the Usage Guidelines.
	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.
	<i>static-group-address</i>	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 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 On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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 None

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 None

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 SSH server status in the running-config.

Synopsis **show running-config ldap-server** [**host** *ipaddr* | **host-name**]

Operands	host	Identifies the IPv4 address of the host.
	<i>ipaddress</i>	IPv4 address of the host.
	host-name	Name of the host.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of the LDAP server in the running-config.

Usage Guidelines LDAP server configuration is placed at the beginning of the running-config and is part of the global configuration of the switch. LDAP is enabled by default and no entry is shown in the running-config when set to default.

Attributes with default values will not be displayed.

Examples Standalone mode

```
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
!
switch#
```

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 None

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 raslog console INFO
logging auditlog class SECURITY
logging auditlog class CONFIGURATION
logging auditlog class FIRMWARE
logging syslog-facility local LOG_LOCAL7
```

SW0#See Also **show running-config logging auditlog class, 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 raslog**

Operands None

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 raslog  
logging 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 mac-address-table

Displays configuration information about MAC interfaces and configurations.

Synopsis **show running-config monitor mac-address-table [aging-time | static]**

Operands **aging-time** Specifies the aging time value (in seconds).
 static Specifies a static MAC address.

Defaults Default aging time is 300 seconds.

Command Modes Privileged EXEC mode

Description Use this command to display configuration information about MAC interfaces and configurations.

Usage Guidelines None

Examples None

See Also None

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 To display the monitor information:

```
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 **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 Brocade VDX 8770-4, VDX 8770-8, and later switches.

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 (global configuration mode), show port-profile, show running-config port-profile activate, show running-config port-profile, 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-domain

2 show running-config port-profile activate

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** (global configuration mode)

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 (global configuration mode), 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	<i>name</i>	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 [<i>name</i>]	The configured QoS CEE map.
	qos	The QoS profile.
	cos <i>cos</i>	The configured default class of service (CoS).
	cos-mutation <i>name</i>	The applied Cos-to-Cos mutation map.
	cos-traffic-class <i>name</i>	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 Layer 2 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** (global configuration mode), **qos cos**, **qos cos-mutation**, **qos map cos-traffic-class**, **qos flowcontrol tx rx**, **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	<i>name</i>	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.
	<i>acl-name</i>	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** (global configuration mode), **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 (global configuration mode)**

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_id*]] | **mode** [**access** | **trunk**] | **trunk** [**allowed** [**vlan** [**add** [*vlan_id*] | **all** | **except** *vlan_id* | **none** | **remove** [*vlan_id*]] | **native-vlan** *vlan_id*]]]

Operands	<i>name</i>	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	Specifies the configured switching characteristics of the Layer 2 interfaces.
	access	Specifies VLAN interfaces for which access is configured for the VLAN profile mode.
	vlan <i>vlan_id</i>	Specifies a VLAN interface configured for access. Refer to the Usage Guidelines.
	mode	Specifies the configured mode of the Layer 2 interface.
	access	Specifies Layer 2 interfaces configured for access mode.
	trunk	Specifies Layer 2 interfaces configured for trunk mode.
	trunk	Specifies Layer 2 interfaces configured for trunk mode.
	allowed	Specifies VLANs that are configured to transmit and receive through the Layer 2 interface.
	vlan add [<i>vlan_id</i>]	Specifies VLANs that are allowed to transmit and receive through the Layer 2 interface.
	vlan all	Specifies all VLANs that are allowed to transmit and receive through the Layer 2 interface.
	vlan except <i>vlan_id</i>	Specifies VLANs that excepted from transmitting and receiving through the Layer 2 interface.
	vlan none	Specifies VLANs that are allowed to transmit and receive through the Layer 2 interface.
	vlan remove [<i>vlan_id</i>]	Specific VLANs to be removed from those allowed to transmit and receive through the Layer 2 interface.
	native-vlan <i>vlan_id</i>	Specifies 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.

2 show running-config port-profile vlan-profile

Usage Guidelines	On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. • On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
Examples	<pre>switch# 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 ! !</pre>
See Also	port-profile (global configuration mode), show running-config port-profile, switchport, switchport access, switchport mode, switchport trunk allowed vlan rspan-vlan, vlan-profile (AMPP)

show running-config port-profile-domain

Displays the port-profile domains and their associated port-profiles.

Synopsis **show running-config port-profile-domain**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the port-profile domains and their associated port profiles.

Usage Guidelines

```
switch# show running-config port-profile-domain
port-profile-domain PP0
    port-profile pp1
    port-profile pp4
!
port-profile-domain PP1
    port-profile pp3
    port-profile pp4
```

Examples None

See Also None

2 show running-config protocol cdp

show running-config protocol cdp

Displays the Cisco Discovery Protocol (CDP) information.

Synopsis **show running-config protocol cdp**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about Cisco Discovery Protocol (CDP).

Usage Guidelines None

Examples None

See Also None

show running-config protocol edge

Displays the Edge Loop Detection (ELD) parameters.

Synopsis **show running-config 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 ELD parameters.

Usage Guidelines None

Examples None

See Also None

show running-config protocol lldp

Displays the Link Layer Discovery Protocol (LLDP) parameters.

Synopsis **show running-config 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 protocol spanning-tree mstp

Displays the protocol configuration information for MSTP.

Synopsis **show running-config protocol spanning-tree mstp** [**bridge-priority** | **cisco-interoperability** | **description** | **error-disable-timeout** | **forward-delay** | **instance** | **max-age** | **max-hops** | **port-channel** | **region** | **revision** | **information** | **shutdown** | **transmit-holdcount** | **vlan**]

Operands	bridge-priority	Displays the Bridge priority commands.
	cisco-interoperability	Displays the Cisco Interoperability status.
	description	Displays the spanning tree description.
	error-disable-timeout	Displays the Error-disable-timeout for the spanning tree.
	forward-delay	Displays the forward delay for the spanning tree.
	hello-time	Displays the hello time settings.
	instance	Displays the MST instance.
	max-age	Displays the max age for the spanning tree.
	max-hops	Displays the MST max hop count.
	port-channel	Displays the status of port-channel for spanning-tree.
	region	Displays the MST region.
	revision	Displays the revision number for configuration information.
	shutdown	Displays the status of the spanning-tree protocol.
	transmit-holdcount	Displays the current transmit hold count of the bridge.
	vlan	Displays the VLAN ID

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the protocol configuration information for MSTP.

Usage Guidelines None

Examples None

See Also **spanning-tree shutdown**

show running-config protocol spanning-tree pvst

Displays the protocol configuration information for PVST.

Synopsis **show running-config protocol spanning-tree pvst** [**bridge-priority** | **cisco-interoperability** | **description** | **error-disable-timeout** | **forward-delay** | **instance** | **max-age** | **max-hops** | **port-channel** | **region** | **revision** | **information** | **shutdown** | **transmit-holdcount** | **vlan**]

Operands	bridge-priority	Displays the Bridge priority commands.
	description	Displays the spanning tree description.
	error-disable-timeout	Displays the Error-disable-timeout for the spanning tree.
	forward-delay	Displays the forward delay for the spanning tree.
	hello-time	Displays the hello time settings.
	max-age	Displays the max age for the spanning tree.
	port-channel	Displays the status of port-channel for spanning-tree.
	shutdown	Displays the status of the spanning-tree protocol.
	vlan	Displays the VLAN ID

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the protocol configuration information for PVST.

Usage Guidelines None

Examples None

See Also **spanning-tree shutdown**

show running-config protocol spanning-tree rpvt

Displays the protocol configuration information for RPVST.

Synopsis `show running-config protocol spanning-tree rpvt [bridge-priority | cisco-interoperability | description | error-disable-timeout | forward-delay | instance | max-age | max-hops | port-channel | region | revision | information | shutdown | transmit-holdcount | vlan]`

Operands	bridge-priority	Displays the Bridge priority commands.
	cisco-interoperability	Displays the Cisco Interoperability status.
	description	Displays the spanning tree description.
	error-disable-timeout	Displays the Error-disable-timeout for the spanning tree.
	forward-delay	Displays the forward delay for the spanning tree.
	hello-time	Displays the hello time settings.
	max-age	Displays the max age for the spanning tree.
	port-channel	Displays the status of port-channel for spanning-tree.
	shutdown	Displays the status of the spanning-tree protocol.
	transmit-holdcount	Displays the current transmit hold count of the bridge.
	vlan	Displays the VLAN ID

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the protocol configuration information for RPVST.

Usage Guidelines None

Examples None

See Also `spanning-tree shutdown`

show running-config protocol spanning-tree rstp

Displays the protocol configuration information for RSTP.

Synopsis **show running-config protocol spanning-tree rstp** [**bridge-priority** | **cisco-interoperability** | **description** | **error-disable-timeout** | **forward-delay** | **instance** | **max-age** | **max-hops** | **port-channel** | **region** | **revision** | **information** | **shutdown** | **transmit-holdcount** | **vlan**]

Operands	bridge-priority	Displays the Bridge priority commands.
	description	Displays the spanning tree description.
	error-disable-timeout	Displays the Error-disable-timeout for the spanning tree.
	forward-delay	Displays the forward delay for the spanning tree.
	hello-time	Displays the hello time settings.
	max-age	Displays the max age for the spanning tree.
	port-channel	Displays the status of port-channel for spanning-tree.
	shutdown	Displays the status of the spanning-tree protocol.
	transmit-holdcount	Displays the current transmit hold count of the bridge.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the protocol configuration information for RSTP.

Usage Guidelines None

Examples None

See Also **spanning-tree shutdown**

show running-config protocol spanning-tree stp

Displays the protocol configuration information for STP.

Synopsis **show running-config protocol spanning-tree stp** [**bridge-priority** | **cisco-interoperability** | **description** | **error-disable-timeout** | **forward-delay** | **instance** | **max-age** | **max-hops** | **port-channel** | **region** | **revision** | **information** | **shutdown** | **transmit-holdcount** | **vlan**]

Operands	bridge-priority	Displays the Bridge priority commands.
	description	Displays the spanning tree description.
	error-disable-timeout	Displays the Error-disable-timeout for the spanning tree.
	forward-delay	Displays the forward delay for the spanning tree.
	hello-time	Displays the hello time settings.
	max-age	Displays the max age for the spanning tree.
	port-channel	Displays the status of port-channel for spanning-tree.
	shutdown	Displays the status of the spanning-tree protocol.

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the protocol configuration information for STP.

Usage Guidelines None

Examples None

See Also **spanning-tree shutdown**

show running-config protocol udd

Displays the UDLD global parameters.

Synopsis **show running-config protocol udd advertise {hello | multiplier | shutdown}**

Operands	hello	Displays the Hello Transmit interval.
	multiplier	Displays the Timeout Multiplier.
	shutdown	Displays the shutdown status.

Defaults This command has no defaults.

Command Modes Privileged EXEC mode

Description Use this command to display information about the UDLD global 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** {*ip-address* | *hostname*}

Operands	host	Identifies the RADIUS server by host name or IP address.
	<i>hostname</i>	Specifies the host name of the RADIUS server.
	<i>ip-address</i>	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 ecmp load-balance**

show running-config rbridge-id linecard

Displays the 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 line cards in the chassis.

Usage Guidelines This command must be executed in the current RBridge ID context.

Examples To display the line card 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 rbridge-id ssh

Displays the Secure Shell (SSH) configuration for an RBridge ID.

Synopsis **show running-config rbridge-id** *rbridge-id* **ssh**

Operands **rbridge-id** *rbridge-id* Specifies the RBridge ID for which to display the SSH configuration.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the SSH configuration for an RBridge ID.

Usage Guidelines None

Examples None

See Also None

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 None

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**

2 show running-config role

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 name, rule, show running-config rule**

show running-config route-map

Displays the status of a route-map application on the specified interface.

Synopsis **show running-config route-map** [*name*]

Operands *name* Specifies the name of the route-map.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the status of a route-map application on the specified interface.

Usage Guidelines There is no need to specify the route map name as the user is only allowed to apply a single route map to an interface.

Examples

```
sw0# show running-config route-map abc
ip policy route-map abc permit 20
   match ip address acl Vincent
   set ip vrf pulp_fiction next-hop 3.3.3.5
   set ip next-hop 4.4.4.4switch#
```

See Also **route-map**

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
<i>index</i>	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 <i>command_name</i>	Displays all rules for the specified command. Type a question mark (?) to display a list of valid commands.
operation { read-only read-write }	Displays the operation for the command.
role <i>role_number</i>	Displays all rules for the specified role.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display configured access rules.

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 name, rule, show running-config rule

show running-config secpolicy

Displays the Switch Connection Control (SCC) security policy information.

Synopsis **show running-config** [**rbridge-id** {*rbridge-id* | **all**}] **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.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
	all	Specifies all identifiers for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the active policy and the defined policy and its policy member set.

Usage Guidelines The **rbridge-id** operand is supported in VCS mode only.

Examples Standalone mode

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 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

```

VCS mode

To show only the defined policy of rbridge-id 3:

```

switch# show running-config rbridge-id 3 secpolicy defined-policy
rbridge-id 3
secpolicy defined-policy SCC_POLICY
member-entry aa:aa:aa:aa:aa:aa:aa:aa
!
member-entry bb:bb:bb:bb:bb:bb:bb:bb
!
member-entry cc:cc:cc:cc:cc:cc:cc:cc
!
!
switch#

```

To show only the active policy of rbridge-id 3:

```

switch# show running-config rbridge-id 3 secpolicy active-policy
rbridge-id 3
secpolicy active-policy SCC_POLICY
member-entry aa:aa:aa:aa:aa:aa:aa:aa
!
member-entry bb:bb:bb:bb:bb:bb:bb:bb
!
member-entry cc:cc:cc:cc:cc:cc:cc:cc
!
!
switch#

```

To show both active and defined policies of rbridge-id 3:

```

switch# show running-config rbridge-id 3 secpolicy
rbridge-id 3
secpolicy defined-policy SCC_POLICY
member-entry aa:aa:aa:aa:aa:aa:aa:aa
!
member-entry bb:bb:bb:bb:bb:bb:bb:bb
!
member-entry cc:cc:cc:cc:cc:cc:cc:cc
!
!
secpolicy active-policy SCC_POLICY
member-entry aa:aa:aa:aa:aa:aa:aa:aa
!
member-entry bb:bb:bb:bb:bb:bb:bb:bb
!
member-entry cc:cc:cc:cc:cc:cc:cc:cc

```

See Also **secpolicy activate, secpolicy defined-policy**

show running-config sflow

Displays the IPv4 and IPv6 addresses and ports of sFlow collectors.

Synopsis **show running-config sflow**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the IPv4 and IPv6 addresses and ports of sFlow collectors.

Usage Guidelines None

Examples To display the IPv4 and IPv6 addresses and ports of sFlow collectors:

```
switch# show running-config sflow
Sflow collector      3ffe:1900:4545:3:200:f8ff:fe21:67cf : 6343
Sflow collector      fe80::200:f8ff:fe21:67cf : 6343
Sflow collector      192.35.41.32 : 6343
```

See Also None

show running-config sflow-policy

Displays the configured sFlow policies.

Synopsis **show running-config sflow-policy**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the configured sFlow policies.

Usage Guidelines None

Examples To display the configured sFlow policies.

```
switch# show running-config sflow-policy
```

See Also None

show running-config sflow-profile

Displays the configured sFlow policies.

Synopsis show running-config sflow-profile

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the configured sFlow profiles.

Usage Guidelines None

Examples None

See Also None

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	This command has no default configurations.
Examples	The following command shows the running configuration of the SNMP server on the switch, with encryption applied: <pre> 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 snmp-server user snmpadmin1 groupname snmpadmin auth md5 auth-password "MVb+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted snmp-server user snmpadmin2 groupname snmpadmin auth md5 auth-password "MVb+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted snmp-server user snmpadmin3 groupname snmpadmin snmp-server user snmpuser2 snmp-server user snmpuser3 auth md5 auth-password "MVb+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password "ckJFoHbzVvhR0xFRPjsMTA==\n" encrypted </pre>
See Also	snmp-server community, snmp-server host, snmp-server contact,snmp-server context,snmp-server location, snmp-server sys-descr, snmp-server user, snmp-server v3host

show running-config snmp-server engineid

Shows the engine ID of the SNMP server on the switch.

Synopsis **show running-config snmp-server engineid**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the engine ID of the SNMP server on the switch.

Usage Guidelines None

Examples To see the engine ID of the SNMP server in standalone mode:

```
switch# show running-config snmp-server engineid  
snmp-server engineID local 10:20:30:40:50:60:70:80:90:10:30:12
```

See Also snmp-server community, snmp-server engineid local, snmp-server host,
snmp-server contact,snmp-server context,snmp-server location, snmp-server sys-descr,
snmp-server user, snmp-server v3host

show running-config ssh

Displays the Secure Shell (SSH) status in the running-config.

Synopsis **show running-config ssh**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the SSH status in the running-config.

Usage Guidelines None

Examples None

See Also None

show running-config ssh server

Displays the SSH server status in the running-config.

Synopsis **show running-config** [**rbridge-id** {*rbridge-id* | **all**}] **ssh server**

Operands	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
	all	Specifies all identifiers for a node.

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 SSH server configuration is placed at the beginning of the running-config and is part of the global configuration of the switch. SSH is enabled by default and no entry is shown in the running-config when set to default.

Examples Standalone mode

```
switch# show running-config ssh server
ssh server shutdown
```

```
switch# show running-config ssh server
ssh server shutdown
ssh server key-exchange dh-group-14
switch#
```

When SSH Server Key-exchange is configured to DH Group 14:

```
switch# show running-config ssh server key-exchange
ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange method has the default value:

```
switch# show running-config ssh server key-exchange
switch#
```

When SSH service is enabled:

```
switch# show run ssh
% No entries found
```

VCS mode

When SSH service is shut down:

```
switch# show running-config rbridge-id 3 ssh server
rbridge-id 3
ssh server shutdown
```

```
switch# show running-config rbridge-id 3 ssh server
rbridge-id 3
ssh server shutdown
ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange is configured to DH Group 14:

```
switch# show running-config rbridge-id 3 ssh server key-exchange
rbridge-id 3
ssh server key-exchange dh-group-14
```

When SSH Server Key-exchange method has the default value:

```
switch# show running-config rbridge-id 3 ssh server key-exchange
rbridge-id 3
```

When SSH service is enabled:

```
switch# show running-config [rbridge-id rbridge-id | all] ssh server
% No entries found
```

See Also **ssh server shutdown, show ssh server status**

2 show running-config ssh server key-exchange

show running-config ssh server key-exchange

Displays the SSH server key-exchange status in the running-config.

Synopsis **show running-config ssh server key-exchange**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of SSH server key-exchange in the running-config.

Usage Guidelines None

Examples Typical command output:

```
switch# show running-config ssh server key-exchange  
ssh server key-exchange dh-group-14
```

See Also **ssh server shutdown, show ssh server status, ssh**

show running-config support

Displays the support parameters in the running configuration.

Synopsis **show running-config support [ffdc]**

Operands **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 ffdc  
support ffdc  
switch#
```

See Also telnet server shutdown, show support

2 show running-config support autoupload-param

show running-config support autoupload-param

Displays autoupload parameters.

Synopsis **show running-config support autoupload-param**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Displays autoupload parameters.

Usage Guidelines None

Examples switch(config)# **do show running-config support autoupload-param**
support autoupload-param hostip 10.31.2.27 username hegdes directory
/users/home40/hegdes/autoupload protocol ftp password
"3iTYxJWEUHp9axZQt2tbvw==\n"
switch(config)#

See Also None

show running-config switch-attributes

Displays switch attributes.

Synopsis **show running-config switch-attributes** [*rbridge-id*] {**chassis-name** | **host-name**}

Operands **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** fec0:60:69bc:94:211:25ff:fec4:6010

To display a single IPv4 TACACS+ server configuration:

switch# **show running-config tacacs-server host** 10.24.65.6

To display a single IPv5 TACACS+ server configuration:

switch# **show running-config tacacs-server host** fec0:60:69bc:94:211:25ff:fec4:6010

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** [**rbridge-id** {*rbridge-id* | **all**}] **telnet server**

Operands **rbridge-id** Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id Specifies a unique identifier for a node.

all Specifies all identifiers for a node.

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 Telnet server configuration is placed at the beginning of running-config and is part of the global configuration of the switch. Telnet is enabled by default and there will be no entry in the running-config when set to default.

Examples Standalone mode

When Telnet service is shut down:

```
switch# show running-config telnet server
telnet server shutdown
```

VCS mode

When Telnet service is shut down:

```
switch# show running-config rbridge-id 3 telnet server
rbridge-id 3
telnet server shutdown
```

When Telnet service is enabled:

```
switch# show running-config [rbridge-id rbridge-id | all] telnet server
% No entries found
```

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	<pre>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</pre> <table><tr><th>Interface</th><th>Area</th><th>Value</th><th>Status</th><th>Monitoring Status</th></tr><tr><td>-----</td><td>-----</td><td>-----</td><td>-----</td><td>-----</td></tr><tr><td>fortygigabitethernet 3/8</td><td>IFG Violation Error</td><td>30</td><td>Out of Range</td><td>Monitoring</td></tr><tr><td>fortygigabitethernet 3/9</td><td>IFG Violation Error</td><td>0</td><td>In Range</td><td>Monitoring</td></tr><tr><td><All other online interfaces></td><td>IFG Violation Error</td><td>0</td><td>In Range</td><td>Monitoring</td></tr></table>	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
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	<pre>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</pre>
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	<i>username</i>	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, Use this command to display all user accounts on the switch.

Use the various 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`, `unlock username`, `username`

show running-config vcs

Displays VCS configuration information.

Synopsis **show running-config vcs [virtual [ip [address]]]**

Operands	virtual	Displays the VCS configuration.
	ip	Displays the virtual IP configuration.
	address	Displays the virtual IP address.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display VCS configuration information.

Usage Guidelines None

Examples None

See Also **vcs (logical chassis cluster mode)**

show running-config zoning

Displays the zoning configuration.

Synopsis **show running-config zoning** [defined-configuration | enabled-configuration]

Operands **defined-configuration** Displays the defined configuration parameters. See **show running-config zoning defined-configuration**.

NOTE

To display the enabled-configuration enabled-zone information, use the **show zoning enabled-configuration** command.

enabled-configuration Displays the enabled configuration parameters. See **show running-config zoning enabled-configuration**.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the zoning configuration for a Brocade VCS Fabric. The base command lists both the defined and the enabled configuration.

Usage Guidelines This command is supported in VCS mode. Zoning configuration data are automatically distributed among all R Bridges in the VCS Fabric. Standalone mode is not supported. For information about enabled zones, refer to the previous Note.

This command can be entered on any R Bridge in a Brocade VCS Fabric.

Examples The following example displays the zoning configuration:

```
switch# show running-config zoning  
zoning defined-configuration cfg cfg1  
    member-zone zone1  
    member-zone zone2
```

See Also **show running-config zoning defined-configuration**,
show running-config zoning enabled-configuration, **show 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 R Bridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any R Bridge 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
!
```

2 show running-config zoning defined-configuration

```
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**]

Operands

cfg-action	Displays the enabled configuration action.
cfg-name	Displays the enabled configuration name.
default-zone-access	Displays the default-zone access mode.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display a variety of information related to the enabled zone configuration.

NOTE

To view details about the enabled zones, use the **show zoning enabled-configuration** command.

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.

Use this command to display the name of the enabled zoning configuration, the configuration action, and the default-zone access mode.

The configuration name is displayed differently depending on two main factors:

- If no transaction is pending, the configuration action is set to “cfg-save.”
- If a transaction is pending, the configuration name is marked with a CFG_MARKER asterisk (*) and the configuration action is set to “cfg-None” The CFG_MARKER flag can also indicate that 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 in VCS Fabric mode.

Zoning configuration data are automatically distributed among all R Bridges in the VCS Fabric.

Standalone mode is not supported.

This command can be executed on any R Bridge in a Brocade VCS Fabric.

Examples To display the enabled zoning configuration:

```
switch# show running-config zoning enabled-configuration
zoning enabled-configuration cfg-name cfg1
zoning enabled-configuration default-zone-access noaccess
zoning enabled-configuration cfg-action cfg-save
```

To display only the default-zone access mode for the enabled zoning configuration:

```
switch# show running-config zoning enabled-configuration default-zone-access
zoning enabled-configuration default-zone-access allaccess
```

2 show running-config zoning enabled-configuration

See Also show running-config zoning, show running-config zoning defined-configuration,
show zoning enabled-configuration

show running-config nas server-ip

Displays information about the specified Auto NAS (automatic network attached storage) interface.

Synopsis **show running-config nas server-ip**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about the specified Auto NAS interface.

Usage Guidelines This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Examples None

See Also **backup-advertisement-interval, clear nas statistics, nas auto-qos, nas server-ip, show nas statistics, show system internal nas, show cee maps**

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 Use this command to display 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** {**fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port*}] | **all**

Operands

all	Displays all sFlow information and statistics.
interface	Displays sFlow information for an Ethernet interface.
fortygigabitethernet	Specifies a valid 40-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
gigabitethernet	Specifies a valid 1-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
tengigabitethernet	Specifies a valid 10-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.

Defaults 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* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display sFlow statistics on the 10-gigabit Ethernet interface 15/0/4:

```
switch# show sflow interface tengigabitethernet 15/0/4
sFlow info for interface Ten Gigabit Ethernet 15/0/4
-----
Configured sampling rate:          100 pkts
Actual sampling rate:              100 pkts
Counter polling interval:         100 secs
Samples received from hardware:    32
Port backoffThreshold :           272
Counter samples collected :        147
```

To display sFlow statistics on 1-gigabit Ethernet interface 22/0/1:

```
switch# show sflow interface gigabitethernet 22/0/1
-----
sFlow info for interface Gigabit Ethernet 22/0/1
Configured sampling rate:          32768 pkts
```

2 show sflow

```
Actual sampling rate:          32768 pkts
Counter polling interval:      20 seconds
Samples received from hardware: 0
Port backoff threshold:        48
-----
```

To display all sFlow statistics:

```
switch# show sflow all
sFlow services are:          enabled
Global default sampling rate: 32768 pkts
Global default counter polling interval: 20 secs
Collector server address      Number of samples sent
-----
3ffe:1900:4545:3:200:f8ff:fe21:67cf : 6343    0
fe80::200:f8ff:fe21:67cf : 6343             0
192.35.41.32: 6343                          0
fe80::201:fdff:fe21:43cd : 6343             0
192.44.23.45: 6343                          0
```

See Also None

show sflow-profile

Displays the sflow profile configurations.

Synopsis **show sflow-profile** {*string* | **all**}

Operands *string* Specifies the name of the profile.
 all Displays all profile information.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the sflow profile configurations.

Usage Guidelines None

Examples None

See Also **sflow enable (global version)**

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 Brocade VDX 8770-4 switches and S1 through S6 for Brocade VDX 8770-8 switches.
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-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).
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 sfp

Displays the SFP breakout configurations.

Synopsis `show sfp [linecard linecard [port port ]]`

Operands `linecard linecard` Specifies line card information.
`port port` Specifies port information.

Defaults Displays the SFP breakout information using a line card. Port number is optional. If absent, all SFP port configurations are shown.

Command Modes Privileged EXEC mode

Description Use this command to display the SFP configuration for the specified line cards. The speed column shows the breakout speed in breakout mode, and the aggregate speed when not in breakout mode.

Usage Guidelines This command is supported on the line cards.

Examples To display the SFP configuration on a line card:

```
switch# show sfp linecard 1
Port  Type      Breakout      Speed
-----
1     SFP         n/a           10G
2     QSFP        4x10G         10G
3     SFP         n/a           40G
4     CSFP        10x10G        100G
```

```
switch# show sfp linecard 1 port 2
Port  Type      Breakout      Speed
-----
2     QSFP        4X10G         10G
```

See Also `clear support`, `copy support`, `show support`, `power-off linecard`, `power-on linecard`, `show running-config hardware connector`

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 Brocade VDX 8770-4 switches, and L1 through L8 on the Brocade VDX 8770-8 switches.

Type Displays the module type. Examples are:

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 40 GbE interface module

27x40G 27-port 40 GbE interface module

6x100G 6-port 100 GbE interface module

Description Module description

ID Module ID. Examples are:

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.

2 show slots

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.

NOTE

An "@" following an SFM status line indicates that the status of the optical switch is "OPEN."

See Also show linecard, show sfm

show spanning-tree

Displays all Spanning Tree Protocol (STP) information.

Synopsis `show spanning-tree [pvst | mst-config | vlan vlan_id]`

Operands

<code>pvst</code>	Spanning-tree PVST+ information.
<code>mst-config</code>	MSTP region configuration information.
<code>vlan vlan_id</code>	Specifies the VLAN number. Refer to the Usage Guidelines.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display all STP information.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

ATTENTION

Brocade Network OS supports PVST+ and Rposting. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Examples None

See Also `show spanning-tree interface`

show spanning-tree brief

Displays the status and parameters of the Spanning Tree Protocol (STP).

Synopsis **show spanning-tree** [**vlan** *vlan_id*] **brief**

Operands **vlan** *vlan_id* Specifies a VLAN. Refer to the Usage Guidelines.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display a summary of the status and parameters of STP 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 switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. When “root guard” is in effect, the **show spanning-tree brief** command output shows the port state as *ERR*, not *root_inc*.

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

2 show spanning-tree brief

Typical output of a summary that contains an rbridge-id as a non-root port.

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

```
Spanning-tree Mode: Rapid Spanning Tree Protocol
```

```
Root ID      Priority 32768
             Address 0005.1ecd.0b8a
             Hello Time 2, Max Age 20, Forward Delay 15
```

```
Root Port   ID : 5/0/22
```

```
Bridge ID    Priority 32768
             Address 0105.3352.6f27
             STP Switch Id: 01e0.5200.0211
             Hello Time 2, Max Age 20,
             Forward Delay 15, Tx-HoldCount 6
             Migrate Time 3 sec
```

Interface	Role	Sts	Cost	Prio	Link-type	Edge
Te 6/0/20	DES	FWD	2000	128	P2P	No
Te 6/0/21	DES	FWD	2000	128	P2P	No
Te 6/0/23	ALT	DSC	2000	128	P2P	No

See Also **show spanning-tree interface, spanning-tree guard root**

show spanning-tree interface

Displays the state of the Spanning Tree Protocol for all named port-channels or 1-gigabit Ethernet, or 10-gigabit Ethernet interfaces.

Synopsis **show spanning-tree interface** [**port-channel** *number* | **fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*]

Operands **port-channel** *number*

Specifies the port-channel number. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.

fortygigabitethernet Specifies a valid 40-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the 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 state of the spanning tree for all named port-channels or 1-gigabit Ethernet, 10-gigabit Ethernet, or 40-gigabit 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* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display information on a 10-gigabit 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)
```

2 show spanning-tree interface

```
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 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 fortygigabitethernet** *rbridge-id/slot/port* | **interface tengigabitethernet** *rbridge-id/slot/port* | **interface gigabitethernet** *rbridge-id/slot/port*]

Operands

interface	Specifies the interface for which to display the MSTP information.
port-channel <i>number</i>	Specifies the port-channel of the interface. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
fortygigabitethernet	Specifies a valid 40-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
tengigabitethernet	Specifies a valid 10-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
gigabitethernet	Specifies a valid 1-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	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* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

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
```

2 show spanning-tree mst detail

```
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 <i>instance_id</i> [interface port-channel <i>number</i> interface fortygigabitethernet <i>rbridge-id/slot/port</i> interface tengigabitethernet <i>rbridge-id/slot/port</i> interface gigabitethernet <i>rbridge-id/slot/port</i>]	
Operands	<i>instance_id</i>	Specifies the MSTP instance for which to display information. Valid values range from 1 through 31.
	interface	Specifies the interface for which to display the MSTP instance information.
	port-channel <i>number</i>	Specifies the port-channel of the interface. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
	fortygigabitethernet	Specifies a valid 40-gigabit Ethernet interface for which to display the MSTP instance information.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet	Specifies a valid 10-gigabit Ethernet interface for which to display the MSTP instance information.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet	Specifies a valid 1-gigabit Ethernet interface for which to display the MSTP instance information.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number for the interface for which to display information on the MSTP instance.
	<i>port</i>	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 <i>rbridge-id/slot/port</i> parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.	
Examples	To display information on MSTP instance 1:	
	<pre>switch# show spanning-tree mst instance 1 interface tengigabitethernet 1/0/0 Instance: 1; VLANs: 100 MSTI Root Id: 8001.0005.1e76.1aa0 (self)</pre>	

2 show spanning-tree mst instance

```
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 <i>number</i>	Specifies the port-channel of the interface. The number of available channels range from 1 through 63 for standalone mode, and from 1 through 6144 for Brocade VCS Fabric mode. However, the channel can be assigned any number from 1 through 6144.
tengigabitethernet	Specifies a valid 10-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number.
<i>port</i>	Specifies a valid port number.
gigabitethernet	Specifies a valid 1-gigabit Ethernet interface.
<i>rbridge-id</i>	Specifies the RBridge ID.
<i>slot</i>	Specifies a valid slot number for the interface for which to display information for the MSTP instance.
<i>port</i>	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* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples To display information for the MSTP interface:

```
switch# show spanning-tree mst interface tengigabitethernet 5/0/1
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
```

2 show spanning-tree mst interface

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 Secure Shell (SSH) server key-exchange status.

Synopsis **show ssh server status** [**rbridge-id** {*rbridge-id* | **all**}]

Operands **rbridge-id** Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id Specifies a unique identifier for a node.

all Specifies all identifiers for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of SSH server.

Usage Guidelines None

Examples Standalone mode

When SSH server is enabled:

```
switch# show ssh server status
Telnet server status: Enabled
```

When SSH server key-exchange method is configured to DH Group 14:

```
switch# show ssh server status
SSH Kex Exchange Algorithm: DH Group 14
```

When SSH server key-exchange method is restored to default:

```
switch# show ssh server status
```

VCS mode

When SSH server is disabled in rbridge-id 3:

```
switch# show ssh server status rbridge-id 3
rbridge-id 3 SSH server status: Enabled
switch#
```

When SSH server key-exchange method is configured to DH Group 14:

```
switch# show ssh server status rbridge-id 3
rbridge-id 3
SSH Kex Exchange Algorithm: DH Group 14
```

When SSH Server Key-exchange method is restored to default

```
switch# show ssh server status rbridge-id 3
rbridge-id 3
```

See Also **ssh server shutdown, show telnet server status, ssh**

2 show ssh server rekey-interval status

show ssh server rekey-interval status

Displays the status information related to the Secure Shell (SSH) server rekey-interval.

Synopsis **show ssh server rekey-interval status**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description This command displays the status information related to the SSH server rekey-interval.

Usage Guidelines None

Examples None

See Also None

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 Enter **show startup-db ?** 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 | ipv6 | mac} *name* **interface** {port-channel *index* | gigabitethernet *slot/port* | tengigabitethernet *slot/port* | fortygigabitethernet *slot/port* | vlan *vlan_id* | ve *vlan_id*} {in | out}

Operands

ip ipv6 mac	Specifies showing the configured rules of either a Layer 2 or Layer 3 ACL.
<i>name</i>	The “name” of the ACL assigned at creation.
port-channel <i>index</i>	Specifies the port-channel index to which the ACL is bound.
gigabitethernet <i>slot/port</i>	Specifies the 1-gigabit Ethernet interface to which the ACL is bound.
tengigabitethernet <i>slot/port</i>	Specifies the 10-gigabit Ethernet interface to which the ACL is bound.
fortygigabitethernet <i>slot/port</i>	Specifies the 40-gigabit Ethernet interface to which the ACL is bound.
vlan <i>vlan_id</i>	Specifies the VLAN interface to which the ACL is bound. Refer to the Usage Guidelines.
ve <i>vlan_id</i>	Specifies the virtual Ethernet (VE) interface to which the ACL is bound. Refer to the Usage Guidelines.
in out	Specifies the ACL binding direction (ingress or egress).

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the statistics of an access-list status or the statistical information on the specified ACL bound to the specified interface.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples Typical output from the basic command.

```
switch# show statistics access-list ip l3ext in ip access-list l3ext
TenGigabitEthernet 1/1/8 in
seq 76 deny ip 10.10.75.10 0.0.0.0 any count log (795239 frames)
seq 77 hard-drop ip 10.10.75.10 0.0.0.0 10.10.11.0 0.0.0.255 count log (0 frames)
seq 78 hard-drop ip any 10.10.11.0 0.0.0.255 count log (0 frames)
seq 79 hard-drop ip any 10.10.0.0 0.0.255.255 count log (0 frames)
seq 80 hard-drop ip 10.10.75.10 0.0.0.0 any count log (0 frames)
```

2 show statistics access-list

```
seq 81 hard-drop ip 10.10.75.0 0.0.0.0 10.10.0.0 0.0.255.255 count log (0 frames)
seq 91 hard-drop ip any any count (0 frames)
seq 100 deny udp 10.10.75.0 0.0.0.255 10.10.76.0 0.0.0.255 count log (0 frames)
seq 1000 permit ip any any count log (0 frames)
```

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** *vlan_id* | **ve** *vlan_id*} {**in** | **out**}

Operands

port-channel *index* Specifies the port-channel index to which the ACL is bound.

gigabitethernet *slot/port* Specifies the 1-gigabit Ethernet interface to which the ACL is bound.

tengigabitethernet *slot/port* Specifies the 10-gigabit Ethernet interface to which the ACL is bound.

fortygigabitethernet *slot/port* Specifies the 40-gigabit Ethernet interface to which the ACL is bound.

vlan *vlan_id* Specifies the VLAN interface to which the ACL is bound. Refer to the Usage Guidelines.

ve *vlan_id* Specifies the virtual Ethernet interface to which the ACL is bound. Refer to the Usage Guidelines.

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

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the statistical information on any ACL of the type specified bound on the specified interface.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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 (Broadcast, Unknown unicast and Multicast)-related configurations in the system.

show storm-control broadcast
Displays all BUM-related configurations in the system for the broadcast traffic type.

show storm-control multicast
Displays all BUM-related configurations in the system for the multicast traffic type.

show storm-control interface type rbridge-id/slot/port
Displays all BUM-related configurations 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 configurations 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 configurations in the system for the specified traffic type. Use this parameter to display information on a per-port basis.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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 10-gigabit Ethernet 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 10-gigabit Ethernet 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

See Also None

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 RBridge ID. This parameter 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” parameter 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 RBridge ID.

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
Ten Gigabit Ethernet 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 internal nas

Displays all NAS server IP addresses in the system.

Synopsis `show system internal nas`

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the specified Auto NAS server IP addresses.

Usage Guidelines This command is supported only on Brocade VDX 8770-4, VDX 8770-8, VDX 6740, and VDX 6740T switches.

Examples To display the IP addresses for all active NAS servers:

```
switch0# show system internal nas
Rbridge 1
-----
Auto-NAS Enabled
Cos 2
Dscp 10
Traffic Class 5
nas server-ip 10.192.100.100/32 vlan 100
nas server-ip 10.192.100.101/32 vrf brown
```

See Also `backup-advertisement-interval`, `clear nas statistics`, `nas auto-qos`, `nas server-ip`, `show nas statistics`, `show running-config nas server-ip`, `show system internal nas`, `show cee maps`

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 using the switch's RBridge ID.
all Reports all RBridge information.

Defaults None

Command Modes RBridge ID configuration 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
```

See Also **show system monitor**, **system-monitor-mail**, **system-monitor**

show telnet server status

Displays the current Telnet server status.

Synopsis **show telnet server status** [**rbridge-id** {*rbridge-id* | **all**}]

Operands	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
	all	Specifies all identifiers for a node.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of Telnet server.

Usage Guidelines None

Examples When Telnet server status is enabled:

```
switch# show telnet server status
Telnet server status: Enabled
```

When Telnet server status is disabled:

```
sw0# show telnet server status
Telnet server status: Disabled
```

If you are in VCS mode

When Telnet server status is enabled:

```
switch# show telnet server status [rbridge-id rbridge-id | all]
Telnet server status: Enabled
```

When Telnet server is disabled in rbridge-id 3:

```
switch# show telnet server status rbridge-id 3
rbridge-id 3 Telnet server status: Disabled

switch#
```

See Also telnet server shutdown, show running-config telnet server

show threshold monitor

Displays the current status of environmental thresholds and alerts for interfaces, security, and SFPs.

Synopsis **show threshold monitor** [**interface all area** | **security area** [**login-violation** [**rbridge-id** *rbridge-id* | **all**] | **telnet-violation** [**rbridge-id** *rbridge-id* | **all**]] | **sfp all area** [**current** | **rxp** | **temperature** | **txp** | **voltage**]

Operands

interface all area	Displays status of interface thresholds and alerts.
security area	Displays status of security thresholds and alerts.
login-violation	Displays status of login violations.
telnet-violation	Displays status of Telnet violations.
sfp all area	Displays status of SFP thresholds and alerts.
current	Amount of current supplied to the SFP transceiver.
rxp	Amount of incoming laser power, in microWatts (μW).
temperature	Temperature of the SFP, in degrees Celsius.
txp	Amount of outgoing laser power, in microWatts (μW).
voltage	Amount of voltage supplied to the SFP.
rbridge-id <i>rbridge-id</i>	Specifies a switch by means of the switch's RBridge ID.
all	Reports status for all nodes in the cluster.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the current status of environmental thresholds and alerts for interfaces, security, and SFPs.

Usage Guidelines None

Examples

```
switch# show threshold monitor security area login-violation rbridge-id all
```

Rbridge-Id	Area	Value	Status	Monitoring Status
154	Login Violation	0	In Range	Monitoring

See Also **show defaults threshold, system-monitor, system-monitor-mail, threshold-monitor**

show tunnel

Displays statistics for tunnels.

Synopsis

```
show tunnel ID [rbridge-id rbridge-id]
show tunnel brief [rbridge-id rbridge-id]
show tunnel dst-ip dst_ip_address brief [rbridge-id rbridge-id]
show tunnel mode vxlan brief [rbridge-id rbridge-id]
show tunnel nsx service-node [rbridge-id rbridge-id]
show tunnel overlay-gateway name brief [rbridge-id rbridge-id]
show tunnel src-ip src_ip_address brief [rbridge-id rbridge-id]
show tunnel statistics [rbridge-id rbridge-id]
```

Operands	tunnel ID	Specifies one tunnel ID for which to show statistics. Range is 1 to 65535.
	<i>rbridge-id</i>	Filters statistics for a specific Rbridge ID.
	brief	Displays brief listings for all tunnels.
	dst-ip <i>dst_ip_address</i>	Filters statistics by tunnel destination IP address.
	mode	Filters statistics by tunnel mode; in Network OS, the only supported mode is vxlan.
	vxlan	Filters statistics on all VXLANs.
	nsx service-node	Filters BUM-enabled tunnels to NSX service nodes.
	overlay-gateway <i>name</i>	Filter by gateway name.
	src-ip <i>src_ip_address</i>	Filters statistics by tunnel source IP address.
	statistics	Displays packet information for all tunnels.

Defaults None

Command Modes Privileged EXEC mode

Description This command lists statistics for all the tunnels in the VCS. The output includes the tunnel ID, source IP address, destination IP address, VRF, administration state, and operational state.

For **show tunnel ID**, details of the specified tunnel are shown. Output includes the tunnel ID, tunnel IF index, administration state, operational state, source IP address, gateway (if any), destination IP address, packet count, byte count, and current outgoing path.

For **show tunnel statistics**, you receive packet information for all tunnels.

Usage Guidelines This command is available only for a switch that is in logical chassis cluster mode.

Examples **Example 1**

To show brief listings for all tunnels in the VCS:

```
sw0# sw0# show tunnel brief
Tunnel 1, mode VXLAN
```



```
Admin state: Up, Oper state: Up
Source IP 100.1.1.11, Vrf default
Destination IP 150.1.1.1

Tunnel 200, mode VXLAN
Admin state: Up, Oper state: Down
Source IP 100.1.1.11, Vrf default
Destination IP 160.1.1.1

Tunnel 300, mode VXLAN
Admin state: Up, Oper state: Up
Source IP 100.1.1.11, Vrf default
Destination IP 170.1.1.1To display statics for VLANs attached to the overlay
gateway:
```

Example 2

To show statistics for the tunnel with the ID of 100:

```
sw0# show tunnel 100
Tunnel 100, mode VXLAN, rbridge-id 1,5-7
Ifindex 100000, Admin state UP, Oper state UP
Overlay gateway: My-GW1
Source IP 100.1.1.11 (Ve 10, VRID 100), Vrf default
Destination IP 200.1.1.1
Outgoing path: <TBD>
Packet count:  TX 10000      RX 2000
Byte count   :  TX 2000000   RX 88333222
```

Example 3

To show high-level statistics for all tunnels:

```
sw0# show tunnel statistics
```

Tunnel ID	Packets		Bytes	
	TX	RX	TX	RX
1	22200	2272	1982888	11000
200	2233	888922	22333	7867822

See Also

show uddld

Shows global UDLD information.

Synopsis **show uddld**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Shows global unidirectional link detection (UDLD) protocol configuration values such as whether the protocol is enabled on the switch and the *hello* time and timeout values.

Usage Guidelines None

Examples To display global UDLD information on the switch:

```
switch# show uddld
UDLD Global Information
  Admin State:          UDLD enabled
  UDLD hello time:      500 milliseconds
  UDLD timeout:         2500 milliseconds
```

See Also **protocol uddld**

show udd interface

Shows UDLD information for interfaces.

Synopsis **show udd interface** [{**fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port*}]

Operands **fortygigabitethernet** *rbridge-id/slot/port*
 Specifies a valid 40-gigabit Ethernet interface for showing UDLD information.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface for showing UDLD information.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface for showing UDLD information.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Shows unidirectional link detection (UDLD) protocol information for one or all ports.

Usage Guidelines The following describes the values that appear in the headings for this command.

Description UDLD headings

Heading	Description
State	Describes if UDLD is enable or disabled.
Mode	Describes if the mode is Receive, Transmit, or Both (Transmit/Receive).
Advertise Transmitted	Describes how often the advertisement is transmitted.
Hold time for advertise	Describes the hold time for receiving devices before discarding.
Re-init Delay Timer	The timer for the reinitializing delay
Tx Delay Timer	The timer for transmission

2 show udd interface

Description UDLD headings

Heading	Description
DCBX Version	The current DCBX version
Auto-Sense	States whether Auto-Sense is active.
Transmit TLVs	Describes what information is being transmitted for the TLV.
DCBX FCoE Priority Bits	Describes the current FCoE priority bit for DCBX.

Examples To display UDLD information for a specific 10-gigabitEthernet interface:

```
switch# show udd interface te 5/0/1
Global Admin State: UDLD enabled

UDLD information for TenGigabitEthernet 5/0/1
  UDLD Admin State: Enabled
  Interface Operational State: Link is down
  Remote hello time: Unknown
  Local system id: 0x1ecd7bfa Remote system id: Unknown
  Local port : 5/0/1 Remote port : Unknown
  Local link id: 0x0 Remote link id: Unknown
  Last Xmt Seq Num: 1 Last Rcv Seq Num: Unknown
```

See Also protocol udd

show udd statistics

Shows UDLD statistics.

Synopsis **show udd statistics** [**interface** {**fortygigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port*}]

Operands **fortygigabitethernet** *rbridge-id/slot/port*
 Specifies a valid 40-gigabit Ethernet interface for showing statistics.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

gigabitethernet *rbridge-id/slot/port*
 Specifies a valid 1-gigabit Ethernet interface for showing statistics.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

tengigabitethernet *rbridge-id/slot/port*
 Specifies a valid 10-gigabit Ethernet interface for showing statistics.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Shows either all unidirectional link detection (UDLD) protocol statistics or shows the statistics on a specified port.

Usage Guidelines None

Examples To show UDLD statistics on a specific 10-gigabitEthernet interface:

```
switch# show udd statistics interface te 5/0/1
```

See Also protocol udd

show users

Displays the users logged in to the system and locked user accounts.

Synopsis **show users** [**rbridge-id** {*rbridge-id* | **all**}]

Operands **rbridge-id** Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.

rbridge-id Specifies a unique identifier for a node.

all Specifies all identifiers for a node.

Defaults None

Command Modes Privileged EXEC mode
RBridge ID 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 rbridge-id all
**USER SESSIONS**
RBridge ID      Username  Role   Device  Time Logged In
195             admin    admin  Cli     2014-01-15 15:11:26
**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 **Example 1**

To display the VCS summary view for a switch that is in fabric cluster mode ("Local-Only"):

```
switch# show vcs
```

```
Config Mode      : Local-Only
VCS ID           : 1
Total Number of Nodes      : 1
Rbridge-Id  WWN                Management IP   VCS Status  Fabric Status  HostName
1           10:00:00:05:33:51:63:42* 10.17.37.154 Online       Online        sw0
```

To display the VCS configuration details:

```
switch# show vcs detail
```

```
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*
```

2 show vcs

```

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)

```

Example 2

To display the VCS summary view for a switch (called *rb1*) that is in logical chassis cluster mode ("Distributed"):

```

rb1# show vcs
Config Mode      : Distributed
VCS ID           : 300
VCS GUID         : 1001bffd-24f5-4a11-8adf-d00991dcae48
Total Number of Nodes : 3

```

Rbridge-Id	WWN	Management IP	Status	HostName
1	10:00:00:05:1E:CD:22:6A*	10.17.10.21	Online	rb1
2	>10:00:00:05:1E:CD:11:6A	10.17.10.22	Online	rb2
3	10:00:00:05:33:00:6C:80	10.17.10.23	Online	sw0

To display the VCS configuration details:

```

rb1# show vcs detail
Config Mode      : Distributed
VCS ID           : 300
VCS GUID         : 1001bffd-24f5-4a11-8adf-d00991dcae48
Total Number of Nodes : 3
Nodes Disconnected from Cluster : 0
Cluster Condition : Good
Cluster Status    : All Nodes Present in the Cluster
Node :1
  Serial Number   : BKH0322F01L
  Condition       : Good
  Status          : Connected to Cluster
  VCS Id          : 300
  Rbridge-Id      : 1*
  Co-ordinator    : NO
  WWN             : 10:00:00:05:1E:CD:22:6A
  Switch MAC      : 00:05:1E:CD:22:6A

```



```

FCF MAC           : 00:05:1E:CD:22:6A
Switch Type       : VDX6720-24
Firmware Ver      : v4.0.0pkadu_nos4.0.0_pit_a_03_0425_01133_att1
Internal IP       : 127.1.0.1
Management IP     : 10.17.10.21
Node :2
Serial Number     : BKH0322F01Y
Condition         : Good
Status           : Co-ordinator
VCS Id           : 300
Rbridge-Id       : 2
Co-ordinator      : YES
WWN              : 10:00:00:05:1E:CD:11:6A
Switch MAC       : 00:05:1E:CD:11:6A
FCF MAC         : 00:05:1E:CD:11:6A
Switch Type     : VDX6720-24
Firmware Ver    : v4.0.0pkadu_nos4.0.0_pit_a_03_0425_01133_att1
Internal IP     : 127.1.0.2
Management IP   : 10.17.10.22
Node :3
Serial Number   : BKH0320F005
Condition       : Good
Status         : Connected to Cluster
VCS Id        : 300
Rbridge-Id    : 3
Co-ordinator   : NO
WWN           : 10:00:00:05:33:00:6C:80
Switch MAC    : 00:05:33:00:6C:80
FCF MAC      : 00:05:33:00:6C:80
Switch Type  : VDX6720-24
Firmware Ver : v4.0.0pkadu_nos4.0.0_pit_a_03_0425_01133_att1
Internal IP  : 127.1.0.3
Management IP : 10.17.10.23

```

Example 3

To issue the **show vcs** command on a VCS-disabled switch:

```

switch# show vcs
state      : Disabled

```

Example 4

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 (standalone mode)**

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.
	<i>rbridge-id</i>	Specifies the RBridge ID 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, Use this command to display 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         4.1.0                               STANDBY
        4.1.0
M2     NOS         4.1.0                               ACTIVE*
```

```

          4.1.0
L1/0   NOS   4.1.0           ACTIVE
          4.1.0
L1/1   NOS   4.1.0           STANDBY
          4.1.0
L2/0   NOS   4.1.0           ACTIVE
          4.1.0
L2/1   NOS   4.1.0           STANDBY
          4.1.0

```

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	4.1.0	STANDBY
		4.1.0	
M2	NOS	4.1.0	ACTIVE*
		4.1.0	
L1/0	NOS	4.1.0	ACTIVE
		4.1.0	
L1/1	NOS	4.1.0	STANDBY
		4.1.0	
L2/0	NOS	4.1.0	ACTIVE
		4.1.0	
L2/1	NOS	4.1.0	STANDBY
		4.1.0	

See Also **firmware download, show firmwaredownloadstatus**

show virtual-fabric status

Displays the status of the Virtual Fabric (VF): VF-capable, VF-incapable, or VF-enabled.

Synopsis	show virtual-fabric status										
Operands	None										
Defaults	None										
Command Modes	Privileged EXEC mode										
Description	Use this command to display the status of the VF with respect to all nodes in the fabric. The possible states are as follows: • VF-capable: All nodes in the fabric can support service or transport VFs. • VF-incapable: At least one node in the fabric cannot support service or transport VFs. • VF-enabled: The Virtual Fabric is already enabled and service or transport VFs are supported										
Usage Guidelines	None										
Examples	Typical command output display. <pre>switch# show virtual-fabric status</pre> Fabric is virtual-fabric incapable <table><thead><tr><th>Rbridge-Id</th><th>Virtual-fabric status</th></tr></thead><tbody><tr><td>1</td><td>capable</td></tr><tr><td>2</td><td>capable</td></tr><tr><td>3</td><td>incapable</td></tr><tr><td>4</td><td>capable</td></tr></tbody></table>	Rbridge-Id	Virtual-fabric status	1	capable	2	capable	3	incapable	4	capable
Rbridge-Id	Virtual-fabric status										
1	capable										
2	capable										
3	incapable										
4	capable										
See Also	None										

show vlan

Displays information about a specific VLAN interface.

Synopsis `show vlan [vlan_id | brief [provisioned | unprovisioned] | classifier]`

Operands

<code>vlan_id</code>	Specifies the VLAN interface to display. Refer to “the Usage Guidelines.
<code>brief</code>	Displays VLAN information for all interfaces including static and dynamic.
<code>classifier</code>	Displays all VLAN classification information. provisioned Displays provisioned VLANs.
unprovisioned	Displays unprovisioned VLANs.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display information about VLANs.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples The following example displays information about an 802.1Q VLAN:

```
switch# show vlan 1
VLAN      Name                State    Ports
                                     (u)-Untagged, (t)-Tagged
                                     (c)-Converged
=====
1          default         ACTIVE   Te 0/0(t)
                                     Te 0/8(t)
                                     Po 1(t)
```

- The following example shows all VLANs that are configured, provisioned (active) and unprovisioned (inactive):

```
switch# show vlan brief
Total Number of VLANs configured:    6
Total Number of VLANs unprovisioned: 0
Total Number of VLANs provisioned:   6
VLAN      Name                State  Ports                Classification
(F)-FCoE
(T)-Transparent
(R)-RSPAN
=====
300        vlan300             ACTIVE Te 4/0/1(t)
5000(T)    vlan5000             ACTIVE Te 2/0/1/(t) ctag 50, 60, 100-200
Te 4/0/1(t) ctag 50, 60, 100-200
5500(T)    vlan5500             ACTIVE Te 3/0/1/(t) ctag 1, 1002, 4093, 4095
5800        vlan5800             ACTIVE Te 2/0/1(t) ctag 800
6000(T)    vlan6000             ACTIVE Te 4/0/1/(t))
```

- The following example shows only provisioned VLANs:

```
switch# show vlan brief provisioned
Total Number of VLANs configured:    8
Total Number of VLANs unprovisioned: 3
Total Number of VLANs provisioned:   5
VLAN      Name                State  Ports                Classification
(F)-FCoE
(R)-RSPAN
=====
1          default             ACTIVE Te 2/0/5(c)
5000       VLAN5000             ACTIVE Te 2/0/5(t) ctag 100
Te 2/0/6(u) ctag 200
Te 3/0/4(u)
Te 3/0/5(u) mac 0004.0004.0004
6000       VLAN6000             ACTIVE Te 2/0/5(t) ctag 300
Te 3/0/5(u) mac 0002.0002.0002
Te 3/0/5 (u) mac-group 1
Po 10(t) ctag 300
7000       VLAN7000             ACTIVE Te 2/0/5 (t) ctag 400
Te 3/0/5 (u) mac 0006.0006.0006
Te 3/0/5 (u) mac-group 2
1002(F)    VLAN1002             ACTIVE Te 2/0/16(t)
Te 3/0/15(t)
```

- The following example shows only unprovisioned VLANs:

```
switch# show vlan brief unprovisioned
Total Number of VLANs configured:      8
Total Number of VLANs unprovisioned: 3
Total Number of VLANs provisioned:     5
VLAN          Name          State          Ports
(F)-FCoE      (u)-Untagged, (t)-Tagged
(R)-RSPAN     (c)-Converged
=====
2000          VLAN2000      INACTIVE(unprovisioned)
4000          VLAN4000      INACTIVE(unprovisioned)
8000          VLAN8000      INACTIVE(unprovisioned)
```

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. Valid values range from 1 through 16.

interface *group number* Specifies the VLAN classifier interface group number. Valid values range from 1 through 16.

interface port-channel *number* Specifies the VLAN classifier port-channel number. Valid values range from 1 through 63.

rule *number* Specifies the VLAN classifier rule number. Valid values range from 1 through 256.

interface tengigabitethernet Specifies a valid 10-gigabit Ethernet interface.

rbridge-id Specifies the RBridge ID.

slot Specifies a valid slot number.

port Specifies a valid port number.

interface gigabitethernet Specifies a valid 1-gigabit Ethernet interface.

rbridge-id Specifies the 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 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* parameter is used only on Brocade VDX 6710, Brocade VDX 8770-4, and Brocade VDX 8770-8 switches.

Examples None

See Also None

show vlan private-vlan

Displays information about private VLANs.

Synopsis	show vlan private-vlan
Operands	None
Defaults	None
Command Modes	Privileged EXEC mode
Description	Use this command to display information about private VLANs.
Usage Guidelines	None

Examples
Typical command output display.
switch# **show vlan private-vlan**

Primary	Secondary	Type	Ports	Classification
=====	=====	=====	=====	=====
6000		primary	Te 4/1/17(t)	ctag 10
			Te 1/2/17(t)	ctag 10
6000	6001	isolated	Te 4/1/17(t)	ctag 11
			Te 2/0/17(t)	ctag 11
6000	6002	community	Te 4/1/17(t)	ctag 12
			Te 3/1/17(t)	ctag 12
6000	6003	community	Te 4/1/17(t)	ctag 13
			Te 3/1/18(t)	ctag 13

See Also None

show vlan rspan-vlan

Displays information about remote SPAN VLANs.

Synopsis	show vlan rspan-vlan
Operands	None
Defaults	None
Command Modes	Privileged EXEC mode
Description	Use this command to display information about remote SPAN VLANs.
Usage Guidelines	None

Examples

```
sw0(conf-if-te-1/1/34)# do show vlan rspan-vlan
Total Number of VLANs configured      : 3
Total Number of VLANs provisioned     : 2
Total Number of VLANs unprovisioned   : 1
VLAN      Name      State      Ports      Classification
=====
6000 (R)   VLAN6000   INACTIVE(member port down) Te 1/1/34(t) ctag 121
6001 (R)   VLAN6001   INACTIVE(member port down) Te 1/1/34(t) ctag 555
```

See Also rspan-vlan

show vnetwork

Displays virtual assets from the vCenter that are discovered on a Brocade VDX switch.

Synopsis **show vnetwork**

```
[datacenter [id | vcenter] |
dvpgs [datacenter string | name string] {vcenter string} |
dvs [datacenter string | name string] {vcenter string} |
hosts [datacenter string | name string] {vcenter string} |
pgs [datacenter string | name string] {vcenter string} |
vcenter status |
vmpolicy [macaddr [datacenter string | mac mac_address] {vcenter string} |
vms |
vss [datacenter string | name string] {vcenter string}]
```

Operands	datacenter	Displays discovered data centers.
	<i>id</i>	Datacenter ID (a string).
	<i>vcenter</i>	vCenter name (a string).
	dvpgs	Displays distributed virtual port groups.
	datacenter	Selects a datacenter.
	name	Selects a distributed virtual port group.
	vcenter	Selects a vCenter (required).
	dvs	Displays distributed virtual switches.
	datacenter	Selects a datacenter.
	name	Selects a distributed virtual switch name.
	vcenter	Selects a vCenter (required).
	hosts	Displays discovered hosts.
	datacenter	Selects a datacenter.
	name	Selects a host name.
	vcenter	Selects a vCenter (required).
	pgs	Displays discovered standard port groups.
	datacenter	Selects a datacenter.
	name	Selects a standard port group.
	vcenter	Selects a vCenter (required).
	vcenter status	Displays configured vCenter status.
	vmpolicy	Displays association between virtual network interface cards (vNICs) or VM kernel NICs (vmkNICs) and port groups or port profiles.
	macaddr	Displays policies by MAC address.
	datacenter	Selects a datacenter.
	mac	Selects a six-octet MAC address; for example, 00:50:56:8e:00:4b.

2 show vnetwork

vcenter	Selects a vCenter (required).
vms	Displays discovered VMs.
vss	Displays discovered standard virtual switches.
datacenter	Selects a datacenter.
name	Selects a virtual switch.
vcenter	Selects a vCenter (required).

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the virtual assets configured on the vCenter and discovered on the VDX switch.

Usage Guidelines None

Examples

```
switch# show vnetwork ?
Possible completions:
  datacenter Shows discovered datacenters
  diff       Shows vcenter and switch configuration diff
  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
```

```
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 vcenter

show vrf

Displays VRF configuration information.

Synopsis **show vrf**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to view VRF configuration information.

Usage Guidelines None

Examples None

See Also None

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	<i>VRID</i>	The virtual-group ID about which to display information. Valid values range from 1 to 128.
	detail	Displays all session information in detail, including session statistics.
	summary	Displays single line, session-information summaries.
	interface	Displays information for an interface that you specify.
	fortygigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This parameter is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 1-gigabit Ethernet interface
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet <i>rbridge-id/slot/port</i>	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display 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
```

2 show vrrp

```
Interface: Ten Gigabit Ethernet 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: Ten Gigabit Ethernet 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: Ten Gigabit Ethernet 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
  =====
```

See Also None

show zoning enabled-configuration

Displays information about the enabled zoning configuration.

Synopsis **show zoning enabled-configuration**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to display the cfg-name and enabled-zone fields of the enabled zoning configuration for a Brocade VCS Fabric.

Usage Guidelines This command is supported in VCS Fabric mode. Zoning configuration data are automatically distributed among all R Bridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any R Bridge in a Brocade VCS Fabric.

Examples

```
switch# show zoning enabled-configuration
zoning enabled-configuration cfg-name cfg1

zoning enabled-configuration enabled-zone zone1
member-entry 10:00:00:00:00:00:00:01

zoning enabled-configuration enabled-zone zone2
member-entry 10:00:00:00:00:00:00:02

switch# show zoning enabled-configuration | count
Count: 8 lines
```

See Also **show running-config zoning defined-configuration,**
show running-config zoning enabled-configuration

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 R Bridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any R Bridge in a Brocade VCS Fabric, but it is always executed on the principal R Bridge.

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, show zoning enabled-configuration

shutdown

Disables the selected interface.

Synopsis **shutdown**
 no shutdown

Operands None

Defaults The interface is disabled.

Command Modes Interface subtype configuration mode

Description Use this command to disable an interface.

Usage Guidelines Enter **no shutdown** to enable the interface.

Examples To disable a specific 10-gigabit Ethernet interface:

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

To enable a specific 1-gigabit Ethernet interface:

```
switch(config)# gigabitethernet interface 1/0/2  
switch(conf-if-gi-1/0/2)# noshutdown
```

See Also interface, interface ve, show ip interface, show interface

shutdown (UDLD)

Disables the unidirectional link detection (UDLD) protocol on all ports.

Synopsis **shutdown**
 no shutdown

Operands None

Defaults None

Command Modes Protocol UDLD configuration mode

Description Use this command to disable the UDLD protocol on all ports without affecting configuration.

Usage Guidelines The **no shutdown** command unblocks all ports that have been blocked by the UDLD protocol..

Examples To shutdown the UDLD protocol:

```
switch# configure
switch(config)# protocol udld
switch(config-udld)# shutdown
```

See Also **protocol udld**

shutdown (STP)

Disables the Multiple Spanning Tree Protocol (MSTP), Rapid Spanning Tree Protocol (RSTP), the Spanning Tree Protocol (STP), Per Vlan Spanning Tree (PVST), or Rapid PVST(RPVST) globally.

Synopsis **shutdown**
 no shutdown

Operands None

Defaults STP is not enabled as it is not required in a loop-free topology.

Command Modes Protocol Spanning Tree configuration mode

Description Use this command to disable the all versions of STP globally.

Usage Guidelines Enter **no shutdown** to re-enable all versions of 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** *num*
 no shutdown-time *num*

Operands *num* Specifies the number of minutes before a port is re-enabled. Valid values range from 10 through 1440 minutes (10 minutes to 24 hours).

Defaults The default value is 0 minutes.
 The port will not be re-enabled automatically.

Command Modes ELD configuration mode

Description Use this command to set the delay between ELD shutting down a port because it has detected a loop and automatically re-enabling that port.

NOTE

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.

Enter **no shutdown-time** to return to the default value.

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**

slot

Enables or disables the slot.

Synopsis **slot** *number* {**disable** | **enable**}

Operands *number* The slot to control. The valid values are 0 or 1.
 disable Disables the slot.
 enable Enables the slot.

Defaults This command has no defaults.

Command Modes Privileged EXEC mode

Description Use this enable or disable the slot.

Usage Guidelines None

Examples None

See Also None

snmp-server community

Sets or removes the community string and read-write or read-only access for each community.

Synopsis **snmp-server community** *string* [**ro** | **rw**]
no snmp-server community *string* [**ro** | **rw**]

Operands *string* Specifies the community string.
ro | **rw** Sets the read-only or read-write access for each community.

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. The maximum number of SNMP communities supported is 256, which includes the following six default communities.

The following community strings are read-write:

- Secret C0de
- 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**, **host**, **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 Enter **no snmp-server contact** *string* 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 location, snmp-server user, snmp-server v3host**

snmp-server context

	Maps the context name in an SNMPv3 packet's protocol data unit (PDU) to the name of a VPN routing and forwarding (VRF) instance.	
Synopsis	snmp-server context <i>context_name</i> vrf-name <i>vrf_name</i> no snmp-server-context <i>context_name</i> vrf-name <i>vrf_name</i>	
Operands	context	Enables the specification of a variable <i>context_name</i> that can be passed in the SNMP PDU.
	vrf-name	Enables the specification of a variable <i>vrf_name</i> that can be retrieved when an SNMP request is sent with the configured <i>context_name</i> . This variable can be used in SNMP requests for "ipCidrRouteTable."
Defaults	None	
Command Modes	Global configuration mode	
Description	Use this command to create a context and map it to the given VRF. The context-to-VRF mapping is one-to-one and is applicable to all SNMP versions.	
Usage Guidelines	None	
Examples	The following snmp-server context command maps the context name "mycontext" to the VRF name "myvrf." <pre>switch(config)# snmp-server context mycontext vrf-name myvrf</pre> The following snmp-server context command deletes the VRF name "myvrf." <pre>switch(config)# no snmp-server context mycontext vrf-name myvrf</pre> The following snmp-server context command creates the new VRF name "mynewvrf" and maps the context to it. <pre>switch(config)# snmp-server context mycontext vrf-name mynewvrf</pre>	
See Also	show running-config snmp-server , snmp-server community , snmp-server contact , snmp-server location , snmp-server user , snmp-server v3host	

snmp-server engineid local

Configures a user-defined engine ID for the SNMP agent.

Synopsis **snmp-server engineid local** *engine_id*
no snmp-server engineid local

Operands engine_id Specifies the ID of the engine.

Defaults None

Command Modes Global configuration mode (for a standalone switch), RBridge ID configuration mode (for VCS mode).

Description Use this command to configure a user-defined engine ID for the SNMP agent.

Usage Guidelines A switch reboot is necessary for the configured engine ID to become active. Enter the **no snmp-server engineid local** command to remove the configured engine ID from database.

Examples To configure a user-defined engine ID for the SNMP agent in standalone mode:

```
switch(config)# snmp-server engineid local 10:20:30:40:50:60:70:80:90:10:30:12
```

To configure a user-defined engine ID for the SNMP agent in VCS mode:

```
switch (config-rbridge-id-152)# snmp-server engineid local 10:00:00:05:33:51:A8:65:05:33:51:A8
```

To remove the configured engine ID from the database:

```
switch(config)# no snmp-server engineid local  
switch (config-rbridge-id-152)# no snmp-server engineid local
```

See Also **show running-config snmp-server**, **show running-config snmp-server engineid**, **snmp-server community**, **snmp-server contact**, **snmp-server location**, **snmp-server user**, **snmp-server v3host**, **snmp-server context**

snmp-server host

Sets the trap destination IP addresses, version, community string (for v1 and v2c), and destination port for the SNMP server host.

Synopsis **snmp-server host** {**ipv4_host** | **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. Valid port IDs range from 0 through 65535. The default port is 162.

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. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of **none** is specified, all traps are filtered and no RASLog traps are received.

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 between 2 and 16 characters.

The following community strings are read-write:

- Secret C0de
- OrigEquipMfr
- private

The following community strings are read-only:

- public
- common
- ConvergedNetwork

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
switch(config)# snmp-server v3host brocade.com snmpuser3 notifytype informs
engineid 80:00:05:23:01:AC:1A:01:F6 severity-level Info
```

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 context**, **snmp-server host**, **snmp-server location**, **snmp-server sys-descr**, **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 The location string is "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 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 string must be between 4 and 255 characters in length.

Defaults The system description is "Brocade VDX switch".

Command Modes Global configuration mode

Description Use this command to specify the MIB-2 OID description.

Usage Guidelines Enter **no snmp-server sys-descr** to return to the default system description.

Examples To set the system description OID to "Brocade Cluster switch":

 switch(config)# **snmp-server sys-descr "Brocade Cluster switch"**

To restore the system description OID to the default:

 switch(config)# **no snmp-server sys-descr**

See Also **show running-config snmp-server**, **snmp-server community**, **snmp-server contact**,
 snmp-server location, **snmp-server user**

snmp-server user

Creates or changes the attributes of SNMPv3 users.

Synopsis	snmp-server user <i>username</i> [groupname <i>group-name</i>] [auth] { md5 sha } [auth-password <i>string</i> { encrypted }] [priv] { DES AES128 } [priv-password <i>string</i> { encrypted }] no snmp-server user <i>user-name</i>	
Operands	<i>username</i>	The name of the user that connects to the agent. The name must be between 1 and 16 characters long.
	groupname <i>group-name</i>	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 <i>string</i>	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 between 1 and 32 characters long.
	priv	Initiates a privacy authentication level setting session. By default, this parameter is disabled.
	DES	Specifies the DES privacy protocol.
	AES128	Specifies the AES128 privacy protocol.
	priv-password <i>string</i>	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. The privacy password alone cannot be configured. You configure the privacy password with the authentication password.
	encrypted	Used to enter the input for auth/priv passwords as encrypted. The encrypted key should be used only while entering the encrypted auth/priv passwords.
Defaults	Two SNMPv3 user groups are configured, snmpadmin and snmpuser, with default users as follows: • In the snmpadmin group there are three read-write users: snmpadmin1, snmpadmin2, and snmpadmin3. • In the snmpuser group there are three read-only users: snmpuser1, snmpuser2, and snmpuser3. The auth parameter is turned off. The priv parameter is turned off. Encryption is not enabled.	
Command Modes	Global configuration mode	

Description Use this command to configure SNMPv3 users that can be associated with a trap and inform response functionality. To add a new user to either group, one of the default users must be deleted. Optional encryption for **auth-password** and **priv-password** is also provided.

Usage Guidelines Enter **no snmp-server user user-name** to delete a user.

This command may not be successful where encrypted passwords are generated by third-party or open-source tools.

Examples To configure a basic authentication policy:

```
switch(config)# snmp-server user brocade groupname snmpadmin auth md5 user123  
priv priv-password user456
```

To configure plain-text passwords:

```
sw0(config)# snmp-server user snmpadmin1 auth md5 auth-password private123 priv  
DES priv-password public123
```

To configure encrypted passwords:

```
sw0(config)# snmp-server user snmpadmin2 groupname snmpadmin auth md5  
auth-password "MVb+360X3kcfBzug5Vo6dQ==\n" priv DES priv-password  
"ckJFoHbzVvhr0xFRPjsMTA==\n" encrypted
```

See Also show running-config snmp-server, snmp-server community, snmp-server contact, snmp-server host, snmp-server location, snmp-server v3host

snmp-server v3host

Specifies the recipient of the SNMPv3 notification parameter.

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. The default notify type is traps.

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. The default UDP port number is 162.

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. The configured severity level marks the reporting threshold. All messages with the configured severity or higher are displayed. If the severity level of None is specified, all traps are filtered and no RASLog traps are received. The default severity level is *none*.

Defaults None

Command Modes Global configuration mode

Description Use this command to specify the recipient of SNMPv3 notifications.

Usage Guidelines Enter **no snmp-server v3host** [host {ipv4_host | ipv6_host | dns_host}] to remove a host.

Examples The **snmp-server v3host** command is similar to the snmp-server host command.

To configure an IPv4 host address:

```
switch(config)# snmp-server v3host 10.23.23.45 snmpadmin1 severity-level info
```

The following **snmp-server v3host 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 v3host 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
```

See Also show running-config snmp-server, snmp-server community, snmp-server contact, snmp-server host, snmp-server location, snmp-server user

source

Configures the monitoring session.

Synopsis **source** [**fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*] **destination** [**fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*] **direction** [**rx** | **tx** | **both**]

no source [**fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*] **destination** [**fortygigabitethernet** *rbridge-id/slot/port* | **tengigabitethernet** *rbridge-id/slot/port* | **gigabitethernet** *rbridge-id/slot/port*] **direction** [**rx** | **tx** | **both**]

Operands	fortygigabitethernet	Specifies a valid external 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet	Specifies a valid external 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	destination	Use this parameter to specify the interface.
	fortygigabitethernet	Specifies a valid external 40-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	tengigabitethernet	Specifies a valid external 10-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.
	<i>slot</i>	Specifies a valid slot number.
	<i>port</i>	Specifies a valid port number.
	gigabitethernet	Specifies a valid 1-gigabit Ethernet interface.
	<i>rbridge-id</i>	Specifies the RBridge ID. This is not valid in standalone mode.

<i>slot</i>	Specifies a valid slot number.
<i>port</i>	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.

Usage Guidelines The source and destination ports must be in the same port-group on a Brocade VDX 6720-60.
Enter **no source** followed by the identifying parameters to delete the port mirroring connection for the specified interface.

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 subtype configuration mode

Description Use this command to automatically identify the edge port.

Usage Guidelines The port can become an edge port if no Bridge Protocol Data Unit (BPDU) is received.
If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes. Enter **no spanning-tree autoedge** to disable automatic edge detection.

Examples To enable automatic edge detection:

```
switch(config)# interface tengigabitethernet 0/1  
switch(conf-if-te-0/1)# spanning-tree autoedge
```

See Also **protocol spanning-tree**

spanning-tree bpd-mac

Sets the MAC address of the Bridge Protocol Data Unit (BPDU).

Synopsis spanning-tree bpd-mac [0100.0ccc.cccd | 0304.0800.0700]
no spanning-tree bpd-mac [0100.0ccc.cccd | 0304.0800.0700]

Operands 0100.0ccc.cccd Cisco Control Mac
0304.0800.0700 Brocade Control Mac

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to explicitly set the MAC address of the BPDU. This command will only take effect when the protocol is PVST+ or R-PVST+.

If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.Brocade Network OS v4.1.0 supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.

Usage Guidelines Enter no spanning-tree bpd-mac 0100.0ccc.cccd 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*

Operands *cost* Specifies the path cost for the Spanning Tree Protocol (STP) calculations. Valid values range from 1 through 200000000.

Defaults The default path cost is 200000000.

Command Modes Interface subtype configuration mode

Description Use this command to configure the path cost for spanning-tree calculations.

Usage Guidelines Lower path cost indicates a greater chance of becoming root.
If xSTP is enabled over VCS, this command must be executed on all the RBridge nodes.

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 subtype configuration mode

Description Use this command to enable the edge port feature. This command is only for RSTP and MSTP. Use the **spanning-tree portfast** command for STP.

Usage Guidelines If xSTP is enabled over VCS, this command must be executed on all RBridge nodes. 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(config-if-te-0/1)# spanning-tree edgeport
```

To set the edgeport BPDU filter for the port:

```
switch(config-if-te-0/1)# spanning-tree edgeport
switch(config-if-te-0/1)# spanning-tree edgeport bpdu-filter
```

To guard the port against reception of BPDUs:

```
switch(config)# interface tengigabitethernet 0/1
switch(config-if-te-0/1)# spanning-tree edgeport
switch(config-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 a VLAN. Refer to the Usage Guidelines.

Defaults Guard root is disabled.

Command Modes Interface subtype configuration mode

Description Use this command to enable the guard root on the 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 data path. 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.

Usage Guidelines The root port provides the best path from the switch to the root switch.

If xSTP is enabled over VCS, this command must be executed on all RBridge nodes. Enter **no spanning-tree guard root** to disable guard root on the selected interface.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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. Valid values range from 1 through 10.

Defaults 2 seconds.

Command Modes Interface subtype configuration mode

Description Use this command to set the interval time between the BPDUs sent by the root switch. This command is only for MSTP.

Usage Guidelines Changing the **spanning-tree hello-time** affects all spanning-tree instances.
The **max-age** command setting must be greater than the **spanning-tree hello-time** command setting.
If xSTP is enabled over VCS, this command must be executed on all RBridge nodes. Enter **no spanning-tree hello-time** to return to the default setting.

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	<i>instance_id</i>	Specifies the MSTP instance. Valid values range from 1 through 32.
	cost <i>cost</i>	Specifies the path-cost for a port. Valid values range from 1 through 20000000.
	priority <i>priority</i>	Specifies the port priority for a bridge in increments of 16. Valid values range 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 path-cost value is 2000 on a 10-gigabit Ethernet interface.

Command Modes Interface subtype configuration mode

Description Use this command to set restrictions for a port in a particular MSTP instance.

Usage Guidelines Use this command for MSTP-specific configurations.
 If xSTP is enabled over VCS, this command must be executed on all RBridge nodes. Enter **no spanning-tree instance** *instance_id* to remove the instance.

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 (STP).

Synopsis **spanning-tree link-type** [**point-to-point** | **shared**]

Operands **point-to-point** Enables rapid transition.
shared Disables rapid transition.

Defaults The **spanning-tree link-type** is set to **point-to-point**.

Command Modes Interface subtype configuration mode

Description Use this command to specify a link type for STP.

Usage Guidelines This command overrides the default setting of the link type.
 If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

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 subtype configuration mode

Description Use this command to enable the Port Fast feature. This command is the only for the Spanning Tree Protocol (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. BPDU filter prevents the switch from sending BPDU frames on ports that are enabled with portfast. BPDU guard disables all portfast-enabled ports should they ever receive BPDU frames. It does not prevent transmitting of BPDU frames.

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 nontrunking mode. If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

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 edgeport**

spanning-tree priority

Changes an interface's spanning-tree port priority.

Synopsis **spanning-tree priority** *priority*
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.

Defaults The default value is 128.

Command Modes Interface subtype configuration mode

Description Use this command to change an interface's spanning-tree port priority.

Usage Guidelines If xSTP is enabled over VCS, this command must be executed on all the R Bridges.
 Enter **no spanning-tree priority** to return to the default setting.

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 subtype configuration mode

Description Use this command to configure the port from becoming a root port.

Usage Guidelines If xSTP is enabled over VCS, this command must be executed on all the R Bridges.
Enter **no spanning-tree restricted-role** to return to the default setting.

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 subtype configuration mode

Description Use this command to restrict the topology change notification BPDUs sent on the port.

Usage Guidelines Enter **no spanning-tree restricted-tcn** to disable this parameter.
 If xSTP is enabled over VCS, this command must be executed on all the RBridges.

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 in VCS Fabric mode. It is enabled in standalone mode.

Command Modes Interface subtype configuration mode

Description Use this command to disable spanning tree on the interface or VLAN.

- Once all of the interfaces have been configured for a VLAN, you can enable Spanning Tree Protocol (STP) for all members of the VLAN with a single command. Whichever protocol is currently selected is used by the VLAN. Only one type of STP can be active at a time.
- A physical interface (port) can be a member of multiple VLANs. For example, a physical port can be a member of VLAN 1002 and VLAN 55 simultaneously. In addition, VLAN 1002 can have STP enabled and VLAN 55 can have STP disabled simultaneously.

Usage Guidelines If xSTP is enabled over VCS, this command must be executed on all the R Bridges.

Enter **no spanning-tree shutdown** to enable spanning tree on the interface or VLAN.

Vlan 1002 can not be enabled with the **spanning-tree shutdown** command while the device is in VCS Fabric mode.

Examples To disable spanning tree on a specific interface:

```
switch(config)# interface tengigabitethernet 0/1  
switch(conf-if-te-0/1)# spanning-tree shutdown
```

To enable spanning tree on VLAN 1002:

```
switch(config)# interface vlan 1002  
switch(conf-if-vl-1002)# no spanning-tree shutdown
```

See Also **protocol spanning-tree**

spanning-tree vlan

Configures the VLAN identifier for the spanning tree interface.

Synopsis **spanning-tree vlan** *vlan_id*
no spanning-tree vlan

Operands **vlan** *vlan_id* Sets the VLAN identifier for the spanning tree interface. Refer to the Usage Guidelines.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to set the VLAN identifier for the spanning tree interface.

Usage Guidelines If xSTP is enabled over VCS, this command must be executed on all RBridge nodes.

Enter **no spanning-tree vlan** to remove the VLAN setting.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None:

See Also **forward-delay, max-age, show spanning-tree**

speed (Ethernet)

Sets the speed on the Ethernet interface.

Synopsis **speed** {**100** | **1000** | **1000-auto** | **10000** | **auto**}
no speed

Operands	100	Forces the speed to 100 Mbps.
	1000	Forces the speed to 1 Gbps.
	1000-auto	Forces the speed to 1 Gbps AN (802.3 Clause 37 Auto-Negotiation)
	10000	Forces the speed to 10 Gbps.
	auto	Allows the interface to negotiate the speed setting.

Defaults Speed is **auto**.

Command Modes 10 gigabit Ethernet interface subtype configuration mode

Description Use this command to set the speed negotiation value for a specific interface.

Usage Guidelines The speed command is not available for 1-gigabit Ethernet or 40-gigabit Ethernet ports.
Enter **no speed** to return to the default.

Examples To set the speed to 10 Gbps on a specific 10-gigabit Ethernet 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 Speed is **auto**.

Command Modes Fibre Channel interface subtype configuration 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 (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 Speed is 10000

Command Modes Interface subtype configuration mode

Description Use this command to set the speed negotiation value for the interface.

Usage Guidelines The speed command is available only for 10-gigabit Ethernet ports.

Examples None

See Also None

speed (port-channel)

Sets the speed on the port-channel interface.

Synopsis **speed {1000 | 10000 | 40000 | 100000 }**
no speed

Operands	1000	Forces the speed to 1 Gbps.
	10000	Forces the speed to 10 Gbps.
	40000	Forces the speed to 40 Gbps.
	100000	Forces the speed to 100 Gbps. This is available only if the HundredGigabit line card is supported.

Defaults Speed is 10000.

Command Modes Port-channel interface subtype configuration mode

Description Use this command to set the speed negotiation value for a specific port-channel interface.

Usage Guidelines Enter **no speed** to return to the default setting.

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**

spt-threshold

Configures the Shortest Path Tree (SPT) threshold.

Synopsis **spt-threshold** {infinity | *num*}

no spt-threshold

Operands **infinity** Use only the rendezvous point to send packets, do not switch over to SPT.
num Rate (in kilobytes per second) that must be reached before switching to SPT.
Valid values range from 1 through 4294967295.

Defaults Default value is 1.

Command Modes PIM router configuration mode

Description Use this command to specify the rate, in kilobytes per second, data is to be sent through the rendezvous point before switching to SPT for sending packets.

Usage Guidelines Enter **no spt-threshold** to return to the default setting of 1.

Examples To set the SPT threshold interval to 20:

`switch(config-pim-router)# spt-threshold 20`

See Also **router pim**

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 parameter 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 parameter 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 parameter 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
<i>IP Address</i>	Specify the server IP address in IPv4 or IPv6 format.
<i>hostname</i>	Alternately, specify the host name, a string between 1 and 253 characters.

Defaults SSH connects to port 22. See Operands for 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)? 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 key-exchange dh-group-14

Specifies the method used for generating the one-time session keys for encryption and authentication with the Secure Shell (SSH) server.

Synopsis **ssh server key-exchange dh-group-14**
 no ssh server key-exchange dh-group-14

Operands None

Defaults This command is not configured as DH Group 14.

Command Modes Global configuration mode
 RBridge ID configuration mode

Description Use this command to specify the method for generating the one-time session keys for encryption and authentication with the SSH server. For information on DH Group 14, refer to RFC 3526.

You can configure the SSH server key-exchange method to DH Group 14. When the SSH server key-exchange method is configured to DH Group 14, the SSH connection from a remote SSH client is allowed only if the key-exchange method at the client end is also configured to DH Group 14.

Usage Guidelines Enter **no ssh server key-exchange dh-group-14** to restore SSH server key-exchange to the default value.

This command is not distributed across the cluster. The RBridge ID of the node should be used to configure service on individual nodes.

Examples Standalone mode

To set SSH server key-exchange to DH Group 14:

```
switch(config)# ssh server key-exchange dh-group-14
```

To restore the SSH server key-exchange to default value:

```
switch(config)# no ssh server key-exchange dh-group-14
```

VCS mode

To set SSH server key-exchange to DH Group 14:

```
switch(config)# rbridge-id 3  
switch(config-rbridge-id-3)# ssh server key-exchange dh-group-14
```

To restore the SSH server key-exchange to default value:

```
switch(config)# rbridge-id 3  
switch(config-rbridge-id-3)# no ssh server key-exchange dh-group-14
```

See Also **show running-config ssh server, show ssh server status**

ssh server rekey-interval

Configures the Secure Shell (SSH) server rekey-interval.

Synopsis **ssh server rekey-interval** *interval*
 no ssh server rekey-interval

Operands *interval* The value for the rekey interval. Range is from 900 to 3600 seconds.

Defaults None

Command Modes Global configuration mode

Description Use this command to configure the SSH server rekey-interval.

Usage Guidelines Use the **no ssh server rekey-interval** command to remove the rekey-interval.

Examples None

See Also None

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
 RBridge ID configuration mode

Description Use this command to disable SSH service on the switch.

Usage Guidelines Enter **no ssh server shutdown** to enable SSH service. This command is not distributed across the cluster. The RBridge ID of the node should be used to configure service on individual nodes.

Examples Standalone mode

To shut down SSH service:

```
switch(config)# ssh server shutdown
```

To enable SSH service:

```
switch(config)# no ssh server shutdown
```

VCS mode

To shut down SSH service:

```
switch(config)# rbridge-id-3  
switch(config-rbridge-id-3)# ssh server shutdown
```

To enable SSH service:

```
switch(config-rbridge-id-3)# no ssh server shutdown
```

See Also **show running-config ssh server, show ssh server status**

ssh server status

Displays SSH service on the switch.

Synopsis **ssh server status**

Operands None

Defaults None

Command Modes Global configuration mode

Description Use this command to display the SSH service on the switch.

Usage Guidelines None

Examples Typical command output:

```
switch# ssh server status  
SSH Kex Exchange Algorithm: DH Group 14
```

See Also **show running-config ssh server, show ssh server status**

static-network (BGP)

Configures a static BGP4 network, creating a stable network in the core.

Synopsis	static-network no static-network <i>network/mask</i> [distance <i>num</i>]	
Operands	<i>network/mask</i>	Network and mask in CIDR notation.
	<i>num</i>	Administrative distance value for this network. The range is from 1 through 255.
Defaults	The default is 200.	
Command Modes	BGP address-family IPv4 unicast configuration mode	
Description	Use this command to configure a static BGP4 network to the core. While a route configured with this command will never flap unless it is deleted manually, a static BGP4 network will not interrupt the normal BGP4 decision process on other learned routes that are installed in the Routing Table Manager (RTM). Consequently, when there is a route that can be resolved, it will be installed into the RTM.	
Usage Guidelines	Use the no form of the command to restore the defaults.	
Examples	Typical example of this command. <pre>switch(config)# rbridge-id 10 switch(config-rbridge-id-10)# router bgp switch(config-bgp-router)# address-family ipv4 unicast switch(config-bgp-ipv4u)# static-network 10.11.12.0/24 distance 300</pre>	
See Also	route-map	

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 <i>rate</i> parameter 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 <i>rate</i> parameter is in percentage of capacity of the interface. If the traffic on the interface reaches this percentage of capacity, no more traffic (for the traffic type specified) is allowed on the interface.
	<i>rate</i>	Specifies the amount of traffic allowed, either in bits per second or a percentage of the capacity of the interface, depending on which parameter 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.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to limit the amount of broadcast, unknown unicast, and multicast (BUM) ingress traffic on a specified interface. The *shutdown* parameter 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.

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.

2 storm-control ingress

Enter **no storm-control ingress** to disable BUM storm control for a particular traffic type on an interface.

Examples To configure storm control on a 10-gigabit Ethernet 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 10-gigabit Ethernet 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*
 no summary-address

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.

Defaults Summary addresses are not configured.

Command Modes OSPF VRF router configuration mode

Description Use this command to 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 0 and sets the tag to 0. 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 parameter affects only imported, type 5 external routes.

Enter **no summary-address** to disable route summarization.

Examples To configure a summary address of 10.1.0.0 with a mask of 255.255.0.0:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)#router ospf
switch(config-router-ospf-vrf-default-vrf)# summary-address 10.1.0.0 255.255.0.0
```

NOTE

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.

See Also None

support

Enables or disables the first-fault data capture (FFDC).

Synopsis **support ffdc**
 no support ffdc

Operands **ffdc** Enables FFDC.

Defaults FFDC is enabled.

Command Modes Global configuration mode

Description Use this command to enable FFDC.

Usage Guidelines This command is supported only on the local switch.
 This command is not supported on the standby management module.
 Enter **no router ffdc** to disable FFDC. When disabled, the daemon does not capture any data, even when a message with FFDC attributes is logged.

Examples To enable FFDC:
 switch(config)# **support ffdc**
 To disable FFDC:
 switch(config)# **no support ffdc**

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

support autoupload enable

Specifies if support autoupload is enabled or disabled. When set to enabled, the data files are automatically transferred to the configured remote location.

Synopsis **support autoupload enable**
 no support autoupload enable

Operands None

Defaults Support autoupload is disabled by default.

Command Modes Global configuration mode

Description Whenever a core file, FFDC, trace data file occurs, the data files are automatically transferred to the configured remote location if the autoupload feature is enabled.

Usage Guidelines Use the **no** form of this command to disable support autoupload.

Examples To enable autoupload mode:

 `switch(config)# support autoupload enable`

 To disable autoupload mode:

 `switch(config)# no support autoupload enable`

See Also **show running-config support autoupload-param**

support autoupload-param

	Defines autoupload parameters.	
Synopsis	support autoupload-param <i>hostip</i> <i>host-ip</i> user <i>user_acct</i> password <i>password</i> protocol [<i>ftp</i> <i>scp</i> <i>sftp</i>] directory <i>path</i>	
Operands	hostip <i>host-ip</i>	Specifies the IP address of the remote host.
	user <i>user_acct</i>	Specifies the user name to access the remote host.
	password <i>password</i>	Specifies the password to access the remote host.
	protocol <i>FTP</i> <i>SCP</i> <i>SFTP</i>	Specifies the protocol used to access the remote server.
	directory <i>path</i>	Specifies the path to the directory.
	rbridge-id	Enables RBridge ID mode to support Virtual Cluster Switching (VCS) on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
	all	Specifies all identifiers for a node.
Defaults	None	
Command Modes	Global configuration mode	
Description	Use this command to define autoupload parameters.	
Usage Guidelines	None	
Examples	To configure autoupload parameters:	
	<pre>switch(config)# support autoupload-paramhostip 10.31.2.27 protocol [ftp scp sftp]username hegdes directory /uers/home40/hegdes/autoupload password (<string>): *****</pre>	
See Also	None	

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 the attribute is to be set for. Only the local RBridge ID is supported.

chassis-name *string* Sets the switch chassis name. The string must be between 1 and 30 ASCII characters in length.

host-name *string* Sets the switch host name. The string must be between 1 and 30 ASCII characters in length.

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, periods (dots), and underscore characters. Spaces are not permitted.

This command is not supported on the standby management module.

This command is supported only on the local switch.

Enter **no switch-attributes** to restore the default values.

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
```

See Also **show running-config switch-attributes**

switchport

Puts the interface in Layer 2 mode.

Synopsis **switchport**
 no switchport

Operands None

Defaults All Layer 2 interfaces are mapped to default VLAN 1 and the interface is set to access mode.

Command Modes Interface subtype configuration mode

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.

Enter **no switchport** to take the switch out of the Layer 2 mode.

Examples To put a specific 10-gigabit Ethernet 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**
 rspan-vlan

switchport access

Sets the Layer 2 interface as access.

Synopsis **switchport access** {**vlan** *vlan_id* | **rspan-vlan** *vlan_id* | **mac** *HHHH.HHHH.HHHH* | **mac-group** *mac-group-id*}

no switchport access {**vlan** *vlan_id* | **rspan-vlan** *vlan_id* | **mac** *HHHH.HHHH.HHHH* | **mac-group** *mac-group-id*}

Operands **vlan** *vlan_id* Sets the port VLAN (PVID) to the specified *vlan_id*. Refer to the Usage Guidelines. Range is below 4096 for 802.1Q VLANs, and from 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. (See Usage Guidelines, below.)

rspan-vlan *vlan_id* Sets a VLAN ID for RSPAN (Remote Switched Port Analyzer) traffic analysis.

mac *HHHH.HHHH.HHHH* Sets a source MAC address for classifying an untagged VLAN specified by the **vlan** keyword.

mac-group *mac-group-id* (Optional) Specifies a set of MAC addresses. The group of addresses must be established by the global **mac-group** command.

Defaults All Layer 2 interfaces are in access mode and belong to the VLAN ID 1.

Command Modes Interface subtype configuration mode on edge ports

Description Use this command to set the Layer 2 interface as access. In access mode, the interface only allows untagged and priority tagged packets.

In a Virtual Fabrics context, use this command also to configure service or transport VFs on an access port. This allows multiple untagged VLANs on the port by means of SRC MAC classifiers.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches) and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches) and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Enter **no switchport access vlan** to set the PVID to the default VLAN 1.

Examples To set the Layer 2 interface PVID to 100 on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(config-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
```

The following examples illustrate configuration with service or transport VFs in a Virtual Fabrics context.

In global configuration mode, establish a mac-group:

```
switch(config)# mac-group 1
switch(config-mac-group 1)# mac 0002.0002.0002
switch(config-mac-group 1)# mac 0005.0005.0005
switch(config-mac-group 1)# mac 0008.0008.0008
```

In interface configuration mode, ensure that the switchport mode is set to access:

```
switch(config)# int te 2/0/1
switch(config-if-te-2/0/1)# switchport mode access
```

Set the default access VLAN (the default is 1) to 5000 (a classified VLAN):

```
switch(config-if-te-2/0/1)# switchport access vlan 5000
```

Classify an 802.1Q VLAN by means of a source MAC address:

```
switch(config-if-te-2/0/1)# switchport access vlan 200 mac 0002.0002.0002
```

Configure a classified VLAN (> 4095) on the same interface with a MAC address. Frames that do not match the source MAC addresses of 0002.0002.0002 or 0004.0004.0004 are classified into VLAN 5000 (the access VLAN for all untagged frames that do not have MAC address classifications).

```
switch(config-if-te-2/0/1)# switchport access vlan 6000 mac 0004.0004.0004
```

The following errors occur because a MAC address can be classified to only one VLAN on the same interface.

```
switch(config-if-te-2/0/1)# switchport access vlan 7000 mac-group 1
switch(config-if-te-2/0/1)# %Error: Mac-address/Mac-group is overlapping with
another Mac-address/Mac-group configuration on the same port.

switch(config-if-te-3/0/1)# switchport mode access
switch(config-if-te-3/0/1)# switchport access vlan 7000 mac-group 1
switch(config-if-te-3/0/1)# switchport access vlan mac 8000 0008.0008.0008
switch(config-if-te-3/0/1)# %Error: Mac-address/Mac-group is overlapping with
another Mac-address/Mac-group configuration on the same port.
```

See Also **interface, mac-group, rspan-vlan, show vlan, switchport mode, switchport trunk allowed vlan rspan-vlan, switchport**

switchport mode

Sets the mode of the 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 subtype configuration mode

Description Use this command to set the mode of the Layer 2 interface. Access mode assigns the port to a VLAN (refer to the Usage Guidelines). 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 or classified VLAN trunk link. Failure to do so can cause bridging loops and VLAN leaks.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples To set the mode of a specific 10-gigabit Ethernet interface to access:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(config-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 rspan-vlan, switchport**

switchport mode private-vlan

Sets the private VLAN (PVLAN) mode of the Layer 2 interface.

Synopsis `switchport mode private-vlan [host] [promiscuous] [trunk [promiscuous | host]]`

Operands	host	Sets the port mode to host (community or isolated) mode. It accepts the untagged or priority tagged packet, and the outgoing packet is untagged.
	promiscuous	Sets the port mode to promiscuous mode.
	trunk	Sets the port mode to PVLAN trunk port. This port can carry multiple VLANs. The outgoing packets carry all VLANs, except for native VLANs.
	trunk host	Sets the port mode to host (community or isolated) mode. The trunk operand means the outgoing packet will be tagged "accept".
	trunk promiscuous	Sets the trunk to promiscuous mode.

Defaults The port does not have any PVLAN attributes by default.

Command Modes Interface subtype configuration mode

Description Use this command to set the private VLAN mode of the Layer 2 interface. This command assigns the primary Vlan to a promiscuous port (refer to the Usage Guidelines). This command also maps a promiscuous port to selected secondary VLANs. This means only selected VLANs can send packets to this port.

Usage Guidelines All switchport modes are independent from each other, including normal mode (access/trunk) and above private VLAN modes. Based on the default behavior of the port, the new mode automatically overwrites the existing mode by deleting the existing mode (removing any relationship/association) and applying the new mode.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples To set the mode of a specific 10-gigabit Ethernet interface to PVLAN trunk:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport mode private-vlan trunk
```

To set the mode of a specific 10-gigabit Ethernet interface to PVLAN promiscuous (untagged):

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport mode private-vlan promiscuous
```

To set the mode of a specific 10-gigabit Ethernet interface to PVLAN promiscuous (tagged):

```
switch(config)# interface tengigabitethernet 178/0/9  
switch(conf-if-te-178/0/9)# switchport mode private-vlan trunk promiscuous
```

See Also private-vlan, show vlan, switchport access, switchport trunk allowed vlan rspan-vlan, switchport

switchport mode trunk-no-default-native

Configures a port to trunk mode without the implicit creation of default native VLAN 1 in a Virtual Fabrics context.

Synopsis	switchport mode trunk-no-default-native
Operands	None
Defaults	None
Command Modes	Interface subtype configuration mode
Description	Use this command to configure a port to trunk mode without the implicit creation of default native VLAN 1 in a Virtual Fabrics context. This is the fundamental difference between this command and the switch mode trunk command, which implicitly creates VLAN 1 on the port.
Usage Guidelines	When this command is enabled, any ingress tagged or untagged packet is discarded until a switchport classification or native VLAN classification is configured. To disable this functionality, simply issue the no switchport command, or enter a different switchport mode by using the switchport mode access command or the switchport mode trunk command. Port mode change is not allowed when port security is enabled on the interface. The global command dot1q tag native-vlan does not affect the ingress or egress tagging behavior of the native VLAN configured in this mode. The following native VLAN commands are supported in this mode: • switchport trunk native-vlan-untagged • switchport trunk native-vlan-xtagged The following native VLAN commands that are supported in regular trunk mode are NOT supported in this mode: • switchport trunk tag native-vlan • switchport trunk native-vlan On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows: • On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
Examples	Configure a trunk port without a default native VLAN, then explicitly configure the native VLAN. <pre>switch(config)# interface te 2/1/1 switch(config-if-te-2/1/1)# switchport mode trunk-no-default-native switch(config-if-te-2/1/1)# switchport trunk native-vlan-xtagged 1 egress tagged</pre>

See Also switchport trunk native-vlan, switchport trunk native-vlan-untagged, switchport trunk native-vlan-xtagged

switchport port-security

Enables or disables port security on an interface port.

Synopsis **switchport port-security**
 no switchport port-security

Operands None

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to enable or disable port security on an interface port.

Usage Guidelines Use the **no switchport port-security** command to disable port security on the interface.
Port mode change is not allowed when port security is enabled on the interface.

Examples None

See Also None

switchport port-security mac-address

Configures the MAC address option for port security on an interface port.

Synopsis `switchport port-security mac-address address vlan vlan_id`

Operands `mac-address address` Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

`vlan vlan_id` Specifies a VLAN. Refer to the Usage Guidelines.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to configure the MAC address option for port security on an interface port.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also None

switchport port-security max

Configures the maximum number of MAC addresses used for port security on an interface port.

Synopsis **switchport port-security max** *value*
no switchport port-security max

Operands *value* The maximum number of secure MAC addresses. Range is from 1 through 8192.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to configure the maximum number of MAC addresses used for port security on an interface port.

Usage Guidelines None

Examples None

See Also None

switchport port-security oui

Configures an Organizationally Unique Identifier (OUI) MAC address for port security on an interface port.

Synopsis	switchport port-security oui <i>address</i> no switchport port-security oui	
Operands	<i>address</i>	The OUI MAC address from which to accept vendor traffic, in the format xxxx.xxxx.xxxx.
Defaults	None	
Command Modes	Interface subtype configuration mode	
Description	Use this command to configure an OUI MAC address from which the interface will accept traffic. All other addresses are ignored.	
Usage Guidelines	Use the no switchport port-security oui command to disable this option. The use of static secure MAC addresses is not included in OUI-based port security.	
	NOTE OUI-based port security is not supported on Brocade VDX 6710 and VDX 6720 platforms.	
	When you configure the first OUI MAC address on a secure port, traffic floods until the entries are programmed in the hardware.	
Examples	None	
See Also	None	

switchport port-security shutdown-time

Configures the shutdown-time option for port security on an interface port.

Synopsis **switchport port-security shutdown-time** *time*

Operands *time* The amount of time to shut down the interface port, in minutes. Range is from 1 through 15.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to configure the shutdown-time option for port security on an interface port.

Usage Guidelines None

Examples None

See Also None

switchport port-security sticky

Converts dynamic MAC addresses to sticky secure MAC addresses.

Synopsis `switchport port-security sticky mac-address address vlan vlan_id`

Operands `mac-address address` Specifies the MAC address-based VLAN classifier rule used to map to a specific VLAN.

`vlan vlan_id` Specifies a VLAN. Refer to the Usage Guidelines.

Defaults None

Command Modes Interface subtype configuration mode

Description You can configure an interface to convert the dynamic MAC addresses to sticky secure MAC addresses and to add them to the running configuration by enabling sticky learning. When this command is executed on an interface, the interface converts all the dynamic secure MAC addresses, including those that were dynamically learned before sticky learning was enabled, to sticky secure MAC addresses.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also None

switchport port-security violation

Configures the violation response options for port security on an interface.

Synopsis **switchport port-security violation {restrict | shutdown}**

Operands	restrict	Drops packets with unknown source addresses until you remove a sufficient number of secure MAC addresses to drop below the maximum value.
	shutdown	Puts the interface into the error-disabled state for a predetermined amount of time.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to configure the violation response options for port security on an interface.

Usage Guidelines None

Examples None

See Also None

switchport private-vlan association trunk

Assigns a primary private VLAN to private VLAN trunk port.

Synopsis **switchport private-vlan association trunk** *primary_vlan_ID* *secondary_vlan_ID*
no switchport private-vlan association trunk *primary_vlan_ID*
no switchport private-vlan association trunk *primary_vlan_ID* *secondary_vlan_ID*

Operands *primary_vlan_ID* The primary VLAN identification.
secondary_vlan_ID The secondary VLAN identification.

Defaults The port does not have any PVLAN attributes by default.

Command Modes Interface subtype configuration mode

Description This command associates primary VLAN and secondary VLAN to a private VLAN trunk port. Refer to the Usage Guidelines.

Usage Guidelines Multiple PVLAN pairs (Primary VLAN, multiple secondaries) can be specified using this command. Therefore, two **no** versions of this command are used to remove association for one primary VLAN, or remove any trunk association.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples To associate a primary VLAN to PVLAN trunk port, in this example 2 is primary VLAN and 302 is secondary VLAN:

```
switch(conf-if-te-178/0/9)# switchport private-vlan association trunk 2 302
```

To remove a primary VLAN to PVLAN trunk port,

```
switch(conf-if-te-178/0/9)# no switchport private-vlan association trunk 2
```

See Also private-vlan, switchport mode private-vlan, switchport private-vlan mapping

switchport private-vlan host-association

Assigns a secondary and primary VLAN pair to host port.

Synopsis **switchport private-vlan host-association** *primary_vlan_ID secondary_vlan_ID*
no switchport private-vlan host-association

Operands *primary_vlan_ID* The primary VLAN identification. Refer to the Usage Guidelines.
secondary_vlan_ID The secondary VLAN identification.

Defaults The port does not have any PVLAN attributes by default.

Command Modes Interface subtype configuration mode

Description This command associates secondary and Primary VLAN pair a PVLAN host port.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also **private-vlan, switchport mode private-vlan, switchport private-vlan mapping**

switchport private-vlan mapping

Maps primary VLAN and secondary VLAN to a promiscuous port.

Synopsis **switchport private-vlan mapping** *primary_vlan_ID* [**add** | **remove**] *secondary_vlan*
no switchport private-vlan mapping

Operands *primary_vlan_ID* The primary VLAN identification. Refer to the Usage Guidelines.
 add Adds the secondary VLAN to the primary mapping.
 remove Removes the secondary VLAN from the primary mapping.
 secondary_vlan The secondary VLAN identification.

Defaults The port does not have any PVLAN attributes by default.

Command Modes Interface subtype configuration mode

Description This command maps primary VLAN and secondary VLAN to a promiscuous port. This command also maps a promiscuous port to selected secondary VLANs. This means only selected VLAN can send packets to this port.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples None

See Also **private-vlan, switchport private-vlan association trunk, switchport private-vlan mapping**

switchport private-vlan trunk allowed vlan

Adds a VLAN to a private VLAN (PVLAN) trunk port.

Synopsis `switchport private-vlan trunk allowed vlan {all | none | [add | remove | except] vlan_id} ctag ctag}`
`no switchport private-vlan trunk allowed vlan vlan_id`

Operands	all	Allows all VLANs.
	none	Removes all VLANs except for VLAN 1.
	add	Adds a specified VLAN.
	remove	Removes the specified VLAN.
	except	Allows all VLANs except the specified VLAN.
	<code>vlan_id</code>	Specifies a VLAN. Refer to the Usage Guideines.
	ctag ctag	Specifies an incoming C-TAG that is associated with a service or transport VF in a Virtual Fabrics context.

Defaults The port will have default VLAN 1.

Command Modes Interface subtype configuration mode

Description This command adds a VLAN to PVLAN trunk port.

Usage Guidelines Use the **no** form of this command to remove a VLAN or C-TAG from a trunk port.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches) and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches) and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context

For service or transport VFs (VLAN ID 4096 through 8191), the C-TAG cannot be a default VLAN, a reserved VLAN, and FCoE VLAN, or an internal control VLAN.

The following illustrates the configuration of PVLANs for both 802.1Q VLANs and service or transport VFs in a Virtual Fabrics context.

Configure a PVLAN trunk port:

```
switch(config)# int te 4/1
switch(config-if-te-2/0/2)# switchport mode private-vlan trunk
```

Configure 802.1Q VLANs and service or transport VFs in a Virtual Fabrics context:

```
switch(config-if-te-2/0/2)# switchport private-vlan trunk allowed vlan add 400
switch(config-if-te-2/0/2)# switchport private-vlan trunk allowed vlan add 5000
ctag 100
```

Configure service or transport VFs as PVLANs, by using the **switchport private-vlan association** command:

```
switch(config-if-te-2/0/2)# switchport private-vlan association trunk 6000 7000
```



```
switch(config-if-te-2/0/2)# switchport private-vlan association trunk 6000 8000
```

See Also **switchport mode, switchport private-vlan association trunk**

switchport private-vlan trunk native-vlan

Sets native private VLAN (PVLAN) characteristics on a trunk port.

Synopsis **switchport private-vlan trunk native-vlan** *vlan_id*
no switchport private-vlan trunk native-vlan

Operands *vlan_id* Specifies a VLAN to transmit and receive through the Layer 2 interface. Refer to the Usage Guidelines.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to set the native PVLAN characteristics of the Layer 2 trunk interface for classifying untagged traffic.

Usage Guidelines Enter **no switchport trunk native-vlan** to reset the native VLAN to the default setting.

Native VLAN configuration is not supported for a port in private vlan trunk promiscuous mode.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples To set native PVLAN characteristics for a VLAN whose VLAN ID is 120:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(conf-if-te-178/0/9)# switchport private-vlan trunk native-vlan 120
```

See Also **switchport mode private-vlan, switchport private-vlan association trunk, switchport private-vlan trunk allowed vlan**

switchport trunk allowed vlan rspan-vlan

Adds or removes VLANs on a Layer 2 interface in trunk mode.

Synopsis **switchport trunk allowed {vlan | rspan-vlan} {add *vlan_id* {ctag {*id* | *ctag-range*} | all | except *vlan_id* | none | remove *vlan_id*}**

Operands

add <i>vlan_id</i>	Adds a VLAN to transmit and receive through the Layer 2 interface. The VLAN can be an 802.1Q VLAN, an RSPAN VLAN, or a transport VLAN. Refer to the Usage Guidelines.
all	Allows only 802.1Q VLANs to transmit and receive through the Layer 2 interface. This keyword does not apply to classified or transport VLANs.
ctag	Specifies an incoming C-TAG or range of C-TAGs for classified or transport VLANs in a Virtual Fabrics context.
<i>id</i>	C-TAG ID.
<i>range</i>	Range of C-TAG IDs, for example, 100-200, or 10,20,100-200) (applicable only if the VLAN is a transport VLAN.
except <i>vlan_id</i>	Allows only 802.1Q VLANs except the specified VLAN ID to transmit and receive through the Layer 2 interface. Refer to the Usage Guidelines.
none	Allows only 802.1Q VLANs to transmit and receive through the Layer 2 interface. This keyword does not apply to service or transport VFs in a Virtual Fabrics context.
rspan-vlan <i>vlan_id</i>	Selects a VLAN for Remote Switched Port Analyzer (RSPAN) traffic monitoring.
remove <i>vlan_id</i>	Removes a VLAN that transmits and receives through the Layer 2 interface. Refer to the Usage Guidelines.

Defaults None

Command Modes Interface subtype configuration mode

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 switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context. For service or transport VFs (VLAN ID 4096 through 8191), the C-TAG cannot be a default VLAN, a reserved VLAN, and FCoE VLAN, or an internal control VLAN.

A transport VF C-TAG can be any VLAN ID that is not used in other classifications or as a 802.1Q VLAN.

Examples To add the tagged VLAN 100 to a specific 10-gigabit Ethernet interface:

2 switchport trunk allowed vlan rspan-vlan

```
switch(config)# interface tengigabitethernet 178/0/9
switch(config-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(config-if-te-178/0/9)# switchport trunk allowed vlan remove 100
```

The following examples illustrate configuration in a Virtual Fabrics context:

Configure an interface as a trunk switchport.

```
switch(config)# int te 1/0/1
switch(config-if-te-1/0/1)# switchport mode trunk
```

A C-TAG is required for a classified VLAN (VLAN ID from 4096 through 8191):

```
switch(config-if-te-1/0/1)# switchport trunk allowed vlan add 7000
switch(config-if-te-1/0/1)# syntax error: unknown argument
```

Configure a classified VLAN with a C-TAG:

```
switch(config-if-te-1/0/1)# switchport trunk allowed vlan add 5000 ctag 100
switch(config-if-te-1/0/1)# switchport trunk allowed vlan add 6000 ctag 200
```

An 802.1Q vlan specified as a user VLAN cannot be used as a C-TAG in a classified VLAN. The following show conflicts.

- Edge C-TAG 100 is already assigned to VLAN 5000 at the same port:

```
switch(config-if-te-1/0/1)# switchport trunk allow vlan add 8000 ctag 100
switch(config-if-te-1/0/1)# %Error: C-tag is already used.
```

- Edge VLAN 100 is already used as a C-TAG in a classified VLAN:

```
switch(config-if-te-1/0/1)# switchport trunk allow vlan 100
switch(config-if-te-1/0/1)# %%Error: One of the vlans in the range is
configured as a ctag on the same port.
```

```
switch(config-if-te-1/0/1)# switchport trunk allow vlan all
switch(config-if-te-1/0/1)# %%Error: Virtual-fabric vlan classification
configuration exists.
switch(config-if-te-1/0/1)# switchport trunk allow vlan add 888
```

- Edge VLAN 888 was already used in 802.1Q configuration.

```
switch(config-if-te-1/0/1)# switchport trunk allow vlan add 8000 ctag 888
switch(config-if-te-1/0/1)# %Error: Ctag is configured in the allowed range
on this port.
```

See Also **interface, rspan-vlan, show vlan, switchport mode, switchport trunk native-vlan, switchport trunk tag native-vlan, transport-service**

switchport trunk default-vlan

Configures tagged or untagged data traffic that does not match any classification rule on a trunk port, supporting service or transport VFs in a Virtual Fabrics context.

Synopsis **switchport trunk default-vlan** *vlan_id*
no switchport trunk default-vlan *vlan_id*

Operands *vlan_id* Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface. Refer to the Usage Guidelines.

Defaults None

Command Modes Interface subtype configuration mode on a trunk port

Description Use this command to configure tagged or untagged data traffic that does not match any classification rule on a trunk port, supporting service, or transport VFs in a Virtual Fabrics context.

Usage Guidelines On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Enter **no switchport trunk default-vlan** *vlan_id* to remove the default VLAN configuration.

Examples Create a transport VF in a Virtual Fabrics context:

```
switch(config)# interface vlan 6000
switch(config-vlan-6000)# transport-service 60
```

Classify all nonmatching traffic except native VLAN traffic to the transparent default VLAN:

```
switch(config-if-te-2/0/1)# switchport trunk default-vlan 6000
```

See Also **interface**, **show vlan**, **switchport mode**, **switchport trunk allowed vlan** *rspan-vlan*, **switchport trunk tag native-vlan**, **transport-service**

switchport trunk native-vlan

Sets native VLAN characteristics as an 802.1Q VLAN, or, in a Virtual Fabrics context, as service or transport VF on a trunk port, matching tagged or untagged data traffic that does not match a classification rule.

Synopsis **switchport trunk native-vlan** *vlan_id* [**ctag** *id*]
no switchport trunk native-vlan *vlan_id* [**ctag** *id*]

Operands *vlan_id* Adds a VLAN to transmit and receive through the Layer 2 interface. Refer to the Usage Guidelines.

ctag *id* Sets an optional C-TAG for a service or transport VF (VLAN ID > 4095). If not present, the native VLAN is untagged.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to set native VLAN characteristics as an 802.1Q VLAN, or, in a Virtual Fabrics context, as a service or transport VF on a trunk port, matching tagged or untagged data traffic that does not match a classification rule.

Usage Guidelines Note the following:

- For VLAN IDs above 4095, the **ctag** keyword is optional.
- If **ctag** is not used, the native VLAN is untagged and the command is validated against the [**no**] **switchport trunk tag native-vlan** command, which controls the tagging of the native VLAN at the interface level. The **switchport trunk native-vlan** command is accepted only if the configuration set by the **switchport trunk tag native-vlan** command allows untagged packets. For VLAN IDs above 4095, validation against the global command **no vlan dot1q tag native** is not required.
- The native VLAN must accept tagged frames for the **ctag** keyword to apply.
- For 802.1Q VLANs (VLAN ID < 4096), both the interface subtype and global commands that control native VLAN tagging apply to the specified native VLAN.

Use the **no** form of this command to unconfigure the native VLAN. VLAN 1 then becomes the native VLAN.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

For service or transport VFs (VLAN ID 4096 through 8191), the C-TAG cannot be a default VLAN, a reserved VLAN, or an internal control VLAN. An FCoE VLAN ID can be used as a C-TAG provided the interface is not configured for “fcoeport default.”

Enter **no switchport trunk native-vlan** to reset the native VLAN to the default setting

Examples To set native VLAN characteristics for an 802.1Q VLAN whose VLAN ID is 120:

```
switch(config)# interface tengigabitethernet 178/0/9
switch(config-if-te-178/0/9)# switchport trunk native-vlan 120
```

The following illustrates the use of the command in a Virtual Fabrics context:

- Configure an interface as a switchport trunk and set the tagging of the native VLAN at the interface level:

```
switch(config)# int te 2/0/1
switch(config-if-te-2/0/1)# switchport mode trunk
switch(config-if-te-2/0/1)# switchport trunk tag native-vlan
```

- Change the native VLAN from the default of 1 to a classified VLAN (VLAN ID > 4095) and add an optional C-TAG:

```
switch(config-if-te-2/0/1)# switchport trunk native-vlan 5000 ctag 50
```

- Change the new native default VLAN to an 802.1Q VLAN (VLAN ID < 4096):

```
switch(config-if-te-2/0/1)# switchport trunk native-vlan 200
```

- The interface must allow untagged packets for classified native VLANs without a C-TAG:

```
switch(config-if-te-2/0/1)# switchport trunk native-vlan 5000
%%Error: Cannot configure non-dot1q native-vlan without a ctag, when
native-vlan-tagging is enabled.
switch(config-if-te-2/0/1)# no switchport trunk tag native-vlan
switch(config-if-te-2/0/1)# switchport trunk native-vlan 5000
```

See Also **interface**, **transport-service**, **show vlan**, **switchport mode**, **switchport trunk allowed vlan**, **rspan-vlan**, **switchport trunk tag native-vlan**

switchport trunk native-vlan-untagged

Configures a port to accept only untagged packets, and specifies that those packets be egress untagged in a Virtual Fabrics context.

Synopsis **switchport trunk native-vlan-untagged** *vlan_id*
no switchport trunk native-vlan-untagged

Operands *vlan_id* Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface. Refer to the Usage Guidelines.

Defaults None

Command Modes Interface subtype configuration mode on a trunk port

Description Use this command to configure a port to accept only untagged packets, and to specify that those packets be egress untagged in a Virtual Fabrics context. The untagged packets may be classified to an 802.1Q VLAN, a service VF, or a transport VF.

Usage Guidelines This command is supported when the port is in no-default-vlan trunk mode, as enabled by means of the **switchport mode trunk-no-default-native** command.

Use the **no switchport trunk native-vlan-untagged** command to remove the configuration.

Port mode change is not allowed when port security is enabled on the interface.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Examples Configure untagged native VLAN 5000, allow VLAN 6000, and make VLAN 7000 the default VLAN.

```
switch(config)# interface te 2/1/1
switch(config-if-te-2/1/1)# switchport mode trunk-no-default-native
switch(config-if-te-2/1/1)# switchport trunk native-vlan untagged 5000
switch(config-if-te-2/1/1)# switchport trunk add vlan 6000 ctag 100-200
switch(config-if-te-2/1/1)# switchport trunk default-vlan 7000
```

Remove the native VLAN 5000.

```
switch(config-if-te-2/1/1)# no switchport trunk native-vlan-untagged
```

See Also **switchport mode trunk-no-default-native**, **switchport trunk native-vlan-xtagged**

switchport trunk native-vlan-xtagged

Configures a port to accept both tagged and untagged packets, and specifies the egress tagging behavior in a Virtual Fabrics context.

Synopsis **switchport trunk native-vlan-xtagged** *vlan_id* [**ctag** *cvid*] **egress** {**tagged** | **untagged** | **any**}
no switchport trunk native-vlan-xtagged

Operands	<i>vlan_id</i>	Adds a classified VLAN (VLAN ID > 4095) to transmit and receive through the Layer 2 interface. Refer to the Usage Guidelines.
	ctag <i>cvid</i>	Sets an optional C-TAG (802.1Q VLAN ID) for a service or transport VF (VLAN ID > 4095).
	egress	Enables the selection of required tagging options.
	tagged	Specifies packets as tagged.
	untagged	Specifies packets as untagged.
	any	Specifies that packets preserve their ingress encapsulation.

Defaults None

Command Modes Interface subtype configuration mode on a trunk port

Description Use this command to accept both tagged and untagged packets, and to specify the egress tagging behavior in a Virtual Fabrics context.

Usage Guidelines This command is supported when the port is in no-default-vlan trunk mode, as enabled by means of the **switchport mode trunk-no-default-native** command.

Note the following:

- Ingress packets may be classified to an 802.1Q VLAN, a service VF, or a transport VF.
- The native VLAN must accept tagged frames for the **ctag** keyword to apply.
- If the specified VLAN is an 802.1Q VLAN, the **ctag** option is not required.
- If the specified VLAN is an 802.1Q VLAN or a service VF, the **egress** tagging options are **tagged** or **untagged**.
- If the specified VLAN is a transport VF, then the **egress** tagging option must be **any** to preserve the encapsulation of ingress frames.

Use the **no switchport trunk native-vlan-xtagged** command to remove the configuration.

Port mode change is not allowed when port security is enabled on the interface.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

2 switchport trunk native-vlan-xtagged

Examples Configure transport VF 6000 that accepts C-TAG range 100 through 200 and a native VLAN that can be either tagged or untagged.

```
switch(config)# interface te 2/1/1  
switch(config-if-te-2/1/1)# switchport mode trunk-no-default-native  
switch(config-if-te-2/1/1)# switchport trunk native-vlan-xtagged 6000 ctag 10  
egress any  
switch(config-if-te-2/1/1)# switchport trunk allow vlan 6000 ctag 100-200
```

Remove the native VLAN from the transport VF.

```
switch(config-if-te-2/1/1)# no switchport trunk native-vlan-xtagged
```

See Also **switchport mode trunk-no-default-native, switchport trunk native-vlan-untagged**

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 subtype configuration mode

Description Use this command to enable tagging for native traffic on a specific interface.

Usage Guidelines Enter **no switchport trunk tag native** to untag native traffic for a specific interface.

Examples To enable tagging for native traffic on a specific 10-gigabit Ethernet 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 rspan-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 string must be between 1 and 50 ASCII characters in length.

Defaults None

Command Modes Protocol LLDP configuration mode

Description Use this command to set the global system description specific to LLDP.

Usage Guidelines Enter **no system-description** to clear the global LLDP system description.

Examples To set the global system description specific to LLDP:

 switch(conf-lddp) # **system-description Brocade**

See Also **system-name**

system-max

Sets the maximum number of Address Resolution Protocol (ARP) requests that the system will allocate.

Synopsis **system-max arp** *number_of_arps*
no system-max arp

Operands **arp** Enables setting the maximum number of ARP requests.
 number_of_arps An integer value from 0 through 16384.

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command to set the maximum number of ARP requests that the system will allocate.

Usage Guidelines Use the **no** form of this command to disable this feature.

Examples None

See Also None

system-monitor

Manages the monitoring of FRUs and sets a variety of alerts when thresholds are exceeded.

Synopsis	system-monitor {LineCard [alert [action [all email none raslog]] state [all faulty inserted none on removed]] threshold [down-threshold marginal-threshold]] MM [threshold [down-threshold marginal-threshold]] cid-card [alert [action state [all faulty inserted none on removed]] threshold [down-threshold marginal-threshold]] compact-flash [threshold [down-threshold marginal-threshold]] fan [alert [action state [all faulty inserted none on removed]] threshold [down-threshold marginal-threshold]] power [alert [action state [all faulty inserted none on removed]] threshold [down-threshold marginal-threshold]] sfp [alert [action state]] temp [threshold [down-threshold marginal-threshold]]} no system-monitor	
Operands	LineCard	Specifies alerts and thresholds for line cards.
	MM	Specifies thresholds for management modules.
	cid-card	Specifies alerts and thresholds for the chassis ID card.
	compact-flash	Specifies thresholds for the compact flash device.
	fan	Specifies alerts and thresholds for the fans.
	power	Specifies alerts and thresholds for the power supplies.
	sfp	Specifies alerts for the small form-factor pluggable devices.
	temp	Specifies thresholds for the temperature sensors.
	alert	Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.
	action	Specifies the response type.
	all	Specifies that e-mail and RASLog messaging are used.
	email	Specifies that an e-mail message is sent.
	none	Specifies that no message is sent.
	raslog	Specifies RASLog messaging.
	state	Specifies the hardware state to be monitored.
	all	Specifies that all hardware states are monitored.
	faulty	Specifies that hardware is monitored for faults.
	inserted	Specifies that the insertion state of hardware is monitored.
	none	Specifies that no hardware states are monitored.
	on	Specifies that the hardware on/off state is monitored.
	removed	Specifies that the removal of hardware is monitored.

threshold	Specifies the monitoring of thresholds
down-threshold	Specifies an integer value that, when exceeded, indicates when hardware is down.
marginal-threshold	Specifies an integer value that, when exceeded, indicates when hardware is operating marginally.

Defaults For system monitoring defaults, see the “System Monitor” chapter in the *Network OS Administrator’s Guide Supporting Network OS v.4.0.0*.

Command Modes RBridge ID configuration mode

Description Use this command to configure field-replaceable unit (FRU) monitoring and actions. Depending on these configuration settings, a variety of actions are generated when there is a change in FRU state.

Usage Guidelines Use this command in RBridge subconfiguration mode to manage the system health monitoring of individual nodes in a cluster.

Examples

```
switch(config-rbridge-id-154)# system-monitor sfm threshold down-threshold 3  
marginal-threshold 2
```

```
switch(config-rbridge-id-154)# system-monitor cid-card alert state faultyinserted  
action email
```

See Also rbridge-id, show system monitor, system-monitor-mail

system-monitor-mail

Configures Fabric Watch e-mail alerts on the switch.

Synopsis **system-monitor-mail** {**fru** | **interface** | **relay** {*host_ip* | *domain_name*} | **security** | **sfp**} **enable** | *email-id*]

no system-monitor-mail

Operands	fru	Configures e-mail alerts for FRUs.
	interface	Configures e-mail alerts for interfaces.
	relay	Configures the relay host for e-mail to work in a non-DNS environment.
	<i>host_ip</i>	Specifies the IPv4 address of the mail server.
	<i>domain_name</i>	Specifies the domain that corresponds to the e-mail ID.
	security	Configures e-mail alerts for security.
	sfp	Configures e-mail alerts for SFPs.
	enable	Enables or disables e-mail alerts for the above options.
	<i>email-id</i>	Specifies the e-mail address to where the alert will be sent.

Defaults 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 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. Both relay parameters (the host IP address and the domain name) must be configured in a non-DNS environment. In a DNS environment, only the host IP address is required).

Examples

```
switch(config)# system-monitor-mail ?
Possible completions:
  fru          Configure FRU mail settings
  interface    Configure interface mail settings
  relay        Configure relay ip mail settings
  security     Configure security mail settings
  sfp          Configure sfp mail settings

switch(config)# system-monitor-mail fru enable

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  
abc.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 string must be between 1 and 32 ASCII characters in length.

Defaults 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 Enter **no system-name** to delete the name.

Examples To specify a system name for the LLDP:

 switch(conf-lddp) # **system-name Brocade**

See Also **system-description**

table-map (BGP)

Maps external entry attributes into the routing table, ensuring that those attributes are preserved after being redistributed into OSPF.

Synopsis **table-map** *string*
no table-map *string*

Operands *string* Specifies a route map to be whose attributes are to be preserved. Range is from 1 through 63 ASCII characters.

Defaults This option is disabled.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to map external entry attributes into the routing table, ensuring that those attributes are preserved after being redistributed into OSPF. This applies to all peers.

Usage Guidelines Use this command only to set the tag values. Normally, a route map is applied on routes (and therefore the routes are updated) before it is stored in the BGP routing table. Use the **table-map** command to begin the update before the routes are stored in the IP routing table.

Route maps that contain **set** statements change values in routes when the routes are accepted by the route map. For inbound route maps (route maps that filter routes received from neighbors), the routes are changed before they enter the BGP4 routing table. For tag values, if you do not want the value to change until a route enters the IP routing table, you can use a table map to change the value. A table map is a route map that you have associated with the IP routing table. The device applies the **set** statements for tag values in the table map to routes before adding them to the routing table. To configure a table map, you first configure the route map, then identify it as a table map. The table map does not require separate configuration. You can have only one table map.

NOTE

Use table maps only for setting the tag value. Do not use table maps to set other attributes. To set other route attributes, use route maps or filters. To create a route map and identify it as a table map, enter commands such those shown in the first example below. These commands create a route map that uses an address filter. For routes that match the IP prefix list filter, the route map changes the tag value to 100 and is then considered as a table map. This route map is applied only to routes that the device places in the IP routing table. The route map is not applied to all routes. The first example below assumes that IP prefix list p11 has already been configured.

Examples The following illustrates the execution of the **table-map** command in the context discussed in Usage Guidelines:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# route-map TAG_IP permit 1
switch(config-route-map/TAG_IP/permit/1)# match ip address prefix-list p11
switch(config-route-map/TAG_IP/permit/1)# set tag 100
switch(config-route-map/TAG_IP/permit/1)# exit
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# table-map TAG_IP
```

Use the **no** form of the command to remove the table map:

```
switch(config)# rbridge-id 10
```

2 table-map (BGP)

```
switch(config-rbridge-id-10)# router bgp  
switch(config-bgp-router)# address-family ipv4 unicast  
switch(config-bgp-ipv4u)# no table-map TAG_IP
```

See Also **route-map**

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*] [**encryption-level** *value_level*] [**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. Valid values range from 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**.

encryption-level *value_level*
 Designates the encryption level for the shared secret key operation. This operand supports JITC certification and compliance. The range of valid values is from 0 through 7, with 0 being clear text and 7 being the most heavily encrypted.

timeout *secs* **Specifies** the time to wait for the TACACS+ server to respond. The default is 5 seconds.

retries *num* **Specifies** the number of attempts allowed to connect to a TACACS+ server. The default is 5 attempts.

Defaults Refer to the Operands for specific defaults.

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** parameter does not support an empty string.

 Executing the **no** form of the **tacacs-server** command attributes resets the specified attributes to their default values.

NOTE

Before downgrading to a Network OS version that does not support the **encryption-level** keyword, set the value of this keyword to **0**. Otherwise, the firmware download will throw an error that requests this value be set to **0**.

2 tacacs-server

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 delete a 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

tagged-ieee-bpdu-enabled

Activates IEEE BPDU packets.

Synopsis **tagged-ieee-bpdu-enabled**
 no tagged-ieee-bpdu-enabled

Operands None

Defaults None

Command Modes mode

Description Use this command to activate IEEE BPDU packets.

ATTENTION

This command should be enabled when the interface is connected to a switch which sends tagged IEEE bpdu packets.

Usage Guidelines Enter **no tagged-ieee-bpdu-enabled** to disable this feature.
 This command should only be used on edge ports.

Examples None

See Also None

tcp burstrate

Sets the threshold for the burst rate of TCP traffic, and defines the lockout time once that threshold is passed.

Synopsis **tcp burstrate** *packet lockup seconds*
no tcp burstrate

Operands *packet* The maximum number of packets allowed over five seconds. Range is from 1 through 100000.

 lockup seconds Sets the number of seconds to lock up the port. Range is from 1 through 3000.

Defaults This feature is disabled.

Command Modes Global configuration mode

Description To protect against TCP SYN attacks, you can configure the Brocade device to drop TCP SYN packets when excessive numbers are encountered. You can set threshold values for TCP SYN packets that are targeted at the router itself or passing through an interface, and drop them when the thresholds are exceeded.

This command sets the threshold for the burstrate, and defines the lockout time once that threshold is passed.

Usage Guidelines None

Examples None

See Also None

telnet

Establishes a Telnet session to a remote networking device.

Synopsis **telnet** {*IP Address* | *hostname*} [**port-number** *port*]

Operands

<i>IP Address</i>	The server IP address in either IPv4 or IPv6 format.
<i>hostname</i>	The host name (a string between 1 and 63 ASCII characters in length).
port-number <i>port</i>	Specifies the port number in the remote device to connect to. Valid values range from 0 through 65535. For the connection to succeed, a TCP server must be listening for client connections at the specified port.

Defaults 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
 RBridge ID configuration mode

Description Use this command to disable Telnet service on the switch.

Usage Guidelines Enter **no telnet server shutdown** to enable Telnet service. This command is not distributed across a cluster. The RBridge ID of the node should be used to configure service on individual nodes.

Examples Standalone mode

To enable Telnet service on a switch:

```
switch(config)# no telnet server shutdown
```

To shut down Telnet service on a switch:

```
switch(config)# telnet server shutdown
```

VCS mode

To shut down Telnet service on a switch:

```
switch(config)# rbridge-id 3  
switch(config-rbridge-id-3)# telnet server shutdown
```

To enable Telnet service on a switch:

```
switch(config)# rbridge-id 3  
switch(config-rbridge-id-3)# no telnet server shutdown
```

See Also show running-config telnet server, show telnet server status

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. Valid values range from 1 through 512. Specify 0 for infinite length.

monitor Enables terminal monitoring.

timeout *value* Specifies the timeout value in minutes. Valid values range from 0 through 136. Specify 0 to disable timeout.

Defaults The default for **length** is 24.

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.

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

 This command is not available on the standby management module.

 Enter **no terminal** (optionally with a specific parameter) to restore the current terminal settings to default.

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

Configures monitoring of CPU usage of the system and alerts the user when configured thresholds are exceeded.

Synopsis **threshold-monitor cpu** {[**actions** [**none** | **raslog** [(**limit** *limit_when_reached* | **poll** *polling_interval* | **retry** *number_of_retries*)]]}
no threshold-monitor cpu

Operands **actions** Specifies the action to be taken when a threshold is exceeded.

none No action is taken.

raslog Specifies RASLog messaging.

limit Specifies the baseline CPU usage limit as a percentage of available resources.

limit_when_reached
 When the limit set by this parameter is exceeded, a RASLog WARNING message is sent. When the usage returns below the limit, a RASLog INFO message is sent. Valid values range from 0 through 80 percent. The default is 70 percent.

poll Specifies the polling interval in seconds.

polling_interval The range is from 0 through 3600. The default is 120

retry Specifies the number of polling retries before desired action is taken.

number_of_retries
 Range is from 1 through 100. The default is 3.

Defaults Refer to the Operands for specific defaults.

Command Modes RBridge ID configuration mode

Description Use this command to monitor CPU usage and send a RASLog WARNING message when configured thresholds are exceeded.

Usage Guidelines None

Examples `switch(config-rbridge-id-154)# threshold-monitor cpu actions rasloglimit 50 poll110`

See Also `rbridge-id`

threshold-monitor interface

Configures monitoring of port statistics on all external gigabit Ethernet interfaces: 1 GbE, 10 GbE, and 40 GbE.

Synopsis **threshold-monitor interface** {[**apply** *policy_name* | **pause** | **policy** *policy_name*] **type** **Ethernet** **area** [**CRCA****AlignErrors** [**alert** [above [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]] **IFG** [**alert** [above [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]] **MissingTerminationCharacter** [**alert** [above [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]] **SymbolErrors** [**alert** [above [**highthresh-action** [[**all** | **lowthresh-action**] | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**] | **below** [**highthresh-action** [**all** | **email** | **fence** | **none** | **raslog**] | **lowthresh-action** [**all** | **email** | **none** | **raslog**]]] | **threshold** [**buffer** | **high-threshold** | **low-threshold** | **timebase** [**day** | **hour** | **minute** | **none**]]]]]}

no threshold-monitor interface

Operands	apply	Applies a custom policy that has been created by the policy operand.
	pause	Pause monitoring.
	policy	Specifies a policy name for monitoring by means of custom settings, rather than default settings. A policy name is required before additional configurations can be made. This operation is not supported from a secondary node.
	<WORD>	Specifies the name of a custom policy configuration that can be saved and applied by means of the apply operand.
	type Ethernet	Enables gigabit Ethernet interface monitoring.

area	Enables policy configuration. CRCAlignErrors The total number of frames received with either a bad Frame Check Sequence (FCS) or an alignment error.
IFG	The minimum-length interframe gap (IFG) between successive frames is violated. The typical minimum IFG is 12 bytes.
MissingTerminationCharacter	The number of frames that terminate in anything other than the Terminate character.
SymbolErrors	The number of words received as an unknown (invalid) symbol. Large symbol errors indicate a bad device, cable, or hardware.
alert	Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.
above	Enables setting a value for highthresh-action , which specifies the action to be taken when a high threshold is exceeded.
below	Enables setting a value for highthresh-action and lowthresh-action , which specifies the action to be taken when a low threshold is exceeded.all Specifies that email and RASLog messaging are used, and that Port Fencing is applied in the case of highthresh-action only.
email	Specifies that an email message is sent.
fence	Specifies that Port Fencing is applied, which disables the port until further action is taken This is available only for highthresh-action .
none	Specifies that no alert notification or other action (Port Fencing) is taken.
raslog	Specifies RASLog messaging.
limit	Specifies the percent of threshold usage, from 0 through 80. The default is 75.
poll	Specifies the polling interval in seconds, from 0 through 3600. The default is 120.
retry	Specifies the number of polling retries before desired action is taken, from 1 through 100. The default is 3.
threshold	Specifies the values for high, low, buffer, and timebase thresholds. These values are used to trigger different alerts and Port Fencing.
buffer	An integer value.
high-threshold	An integer value.
low-threshold	An integer value.
timebase	Calculates differences between current and previous data taken over a variety of intervals, for comparison against the preset threshold boundary.
day	Calculates the difference between a current data value and that value a day ago.
hour	Calculates the difference between a current data value and that value an hour ago.
minute	Calculates the difference between a current data value and that value a minute ago.

	none	Compares a data value to a threshold boundary level.
Defaults	See Operands.	
Command Modes	RBridge ID configuration mode	
Description	When any monitored error crosses the configured high or low threshold, an alert is generated and a problem port can be taken out of service. Use this command to monitor port statistics on all external gigabit Ethernet interfaces and generate a variety of actions, from alerts through Port Fencing.	
Usage Guidelines	None	
Examples	<pre>switch(config-rbridge-id-154)# threshold-monitor interface policy mypolicy type Ethernet area IFG alert above highthresh-action fence raslog lowthresh-action email raslog</pre>	
See Also	rbridge-id	

threshold-monitor memory

Configures monitoring of the memory usage of the system and alerts the user when configured thresholds are exceeded.

Synopsis **threshold-monitor memory** {[**actions** [**none** | **raslog** (**high-limit** *percent* | **limit** *percent* | **low-limit** *percent* | **poll** *polling_interval* | **retry** *number_of_retries*) | **high-limit** *percent* | **limit** *percent* | **low-limit** *percent* | **poll** *polling_interval* | **retry** *number_of_retries*]}]

no threshold-monitor memory

Operands	actions	Specifies the action to be taken when a threshold is exceeded.
	none	No action is taken. This is the default.
	raslog	Specifies RASLog messaging.
	high-limit	Specifies an upper limit for memory usage as a percentage of available memory.
	<i>percent</i>	This value must be greater than the value set by limit . When memory usage exceeds this limit, a RASLog CRITICAL message is sent. Values range from 0 through 80 percent. The default is 70 percent.
	limit	Specifies the baseline memory usage limit as a percentage of available resources.
	<i>percent</i>	When this value is exceeded, a RASLog WARNING message is sent. When the usage returns below the value set by limit , a RASLog INFO message is sent. Values range from 0 through 80 percent. The default is 60 percent.
	low-limit	Specifies a lower limit for memory usage as percentage of available memory.
	<i>percent</i>	This value must be smaller than the value set by limit . When memory usage exceeds or falls below this limit, a RASLog INFO message is sent. The default is 40 percent.
	poll	Specifies the polling interval in seconds.
	<i>polling_interval</i>	The range is from 0 through 3600. The default is 120
	retry	Specifies the number of polling retries before desired action is taken.
	<i>number_of_retries</i>	Range is from 1 through 100. The default is 3.

Defaults See Operands.

Command Modes RBridge ID 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-rbridge-id-154)# threshold-monitor memory actions none
high-limit 80 low-limit 50 limit 70 retry 2 poll 30`

See Also `rbridge-id`

threshold-monitor security

Configures monitoring of security parameters, such as telnet and login violations.

Synopsis **threshold-monitor security** {[**apply** *policy_name* | **pause** | **policy** *policy_name*] **area**
 [login-violation
 [alert
 [above [highthresh-action [[all | lowthresh-action] | email | fence | none | raslog] |
 lowthresh-action [all | email none | raslog] |
 below [highthresh-action [all | email | fence | none | raslog] | lowthresh-action [all | email |
 none | raslog]] |
 threshold
 [buffer | high-threshold | low-threshold | timebase [day | hour | minute | none]]]
 telnet-violation
 [alert
 [above [highthresh-action [[all | lowthresh-action] | email | fence | none | raslog] |
 lowthresh-action [all | email none | raslog] |
 below [highthresh-action [all | email | fence | none | raslog] | lowthresh-action [all | email |
 none | raslog]] |
 threshold
 [buffer | high-threshold | low-threshold | timebase [day | hour | minute | none]]]]]
no threshold-monitor security

Operands	apply	Applies a custom policy that has been created by the policy operand.
	<i>policy_name</i>	Name of a custom policy configuration created by the policy operand.
	pause	Pauses monitoring.
	policy	Specifies a policy name for monitoring by means of custom settings, rather than default settings. A policy name is required before additional configurations can be made. This operation is not supported from a secondary node.
	<i>policy_name</i>	Name of a custom policy configuration that can be saved and applied by means of the apply operand.
	area	Enables policy configuration.
	login-violation	Enables monitoring of login violations.
	alert	Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.
	above	Enables setting a value for highthresh-action , which specifies the action to be taken when a high threshold is exceeded.
	below	Enables setting a value for highthresh-action and lowthresh-action , which specifies the action to be taken when a low threshold is exceeded.
	all	Specifies that email and RASLog messaging are used, and that Port Fencing is applied in the case of highthresh-action only.
	all	Specifies that email and RASLog messaging are used.
	email	Specifies that an email message is sent.

fence	Specifies that Port Fencing is applied, which disables the port until further action is taken.
none	No alert is sent
raslog	Specifies RASLog messaging.
limit	Specifies the percent of threshold usage, from 0 through 80. The default is 75.
poll	Specifies the polling interval in seconds, from 0 through 3600. The default is 120.
retry	Specifies the number of polling retries before desired action is taken, from 1 through 100. The default is 3.
threshold	Specifies the values for high, low, buffer, and timebase thresholds. These values are used to trigger different alerts and Port Fencing.
buffer	An integer value.
high-threshold	An integer value.
low-threshold	An integer value.
timebase	Calculates differences between current and previous data taken over a variety of intervals, for comparison against the preset threshold boundary.
day	Calculates the difference between a current data value and that value a day ago.
hour	Calculates the difference between a current data value and that value an hour ago.
minute	Calculates the difference between a current data value and that value a minute ago.
none	Compares a data value to a threshold boundary level.
telnet-violation	Enables monitoring of Telnet violations. Operands are as for login-violation .

Defaults See Operands. For other security monitoring defaults, see the “System Monitor” chapter in the *Network OS Administrator’s Guide*.

Command Modes RBridge ID configuration mode

Description Use this command to configure high and low thresholds against which login and telnet violations are compared and alerts are sent.

Usage Guidelines None

Examples Here are examples of typical commands:

```
switch(config-rbridge-id-154)# threshold-monitor security policy mypolicy area
telnet-violation threshold high-threshold 10 buffer 3

switch(config-rbridge-id-154)# threshold-monitor security policy mypolicy area
login-violation timebase hour
```

See Also **rbridge-id**

threshold-monitor sfp

Configures monitoring of SFP parameters.

Synopsis **threshold-monitor sfp** **[[apply policy_name | pause | policy policy_name] type SFP_type area parameters alert**
[above [highthresh-action [[all | lowthresh-action] | email | none | raslog] | lowthresh-action [all | email none | raslog] | below [highthresh-action [all | email | none raslog] | lowthresh-action [all | email | none | raslog]] | threshold [buffer | high-threshold | low-threshold | timebase [day | hour | minute | none]]]]
no threshold-monitor sfp

Operands	apply	Applies a custom policy that has been created by the policy operand.
	policy_name	Name of a custom policy configuration created by the policy operand.
	pause	Pause monitoring.
	policy	Specifies a policy name for monitoring by means of custom settings, rather than default settings. A policy name is required before additional configurations can be made. This operation is not supported from a secondary node.
	policy_name	Name of a custom policy configuration that can be saved and applied by means of the apply operand.
	type	Specifies the SFP type. Possible completions are as follows:
	1GLR	— SFP Type 1GLR
	1GSR	— SFP Type 1GSR
	10GLR	— SFP Type 10GLR
	10GSR	— SFP Type 10GSR
	10GUSR	— SFP Type 10GUSR
	100GSR	—SFP Type 100GSR
	QSFP	— SFP type QSFP
	area	Specifies one of the following SFP parameters to be monitored. See Defaults, below.
	Current	Measures the current supplied to the SFP transceiver.
	RXP	Measures the incoming laser power, in microWatts (µW).
	TXP	Measures the outgoing laser power, in µW).
	Temperature	Measures the temperature of the SFP, in degrees Celsius.
	Voltage	Measures the voltage supplied to the SFP.
	alert	Specifies whether an alert is sent when a threshold value is either above or below a threshold trigger.

above	Enables setting a value for highthresh-action , which specifies the action to be taken when a high threshold is exceeded.
below	Enables setting a value for highthresh-action and lowthresh-action , which specifies the action to be taken when a low threshold is exceeded.all Specifies that email and RASLog messaging are used, and that Port Fencing is applied in the case of highthresh-action only.
all	Specifies that email and RASLog messaging are used.
email	Specifies that an email message is sent.
none	Specifies that no alert is sent.
raslog	Specifies RASLog messaging.
limit	Specifies the percent of threshold usage, from 0 through 80. The default is 75.
poll	Specifies the polling interval in seconds, from 0 through 3600. The default is 120.
retry	Specifies the number of polling retries before desired action is taken, from 1 through 100. The default is 3.
threshold	Specifies the values for high, low, buffer, and timebase thresholds. These values are used to trigger different alerts and Port Fencing.
buffer	An integer value.
high-threshold	An integer value.
low-threshold	An integer value.
timebase	Calculates differences between current and previous data taken over a variety of intervals, for comparison against the preset threshold boundary.
day	Calculates the difference between a current data value and that value a day ago.
hour	Calculates the difference between a current data value and that value an hour ago.
minute	Calculates the difference between a current data value and that value a minute ago.
none	Compares a data value to a threshold boundary level.

Defaults For the default parameter values of the SFP types, refer to the chapter “System Monitor” in *Network OS Administrator’s Guide*.

Command Modes RBridge ID configuration mode

Description Use this command to monitor SFP parameters and alert the user when configured thresholds are exceeded.

Usage Guidelines None

Examples A typical command might look like this:

```
switch(config)# threshold-monitor sfp custom type QSFP area rxp threshold
high-threshold 2000 low-threshold 1000
```

2 threshold-monitor sfp

See Also rbridge-id

timeout fnm

For Access Gateway mode, this sets and displays the fabric name monitoring time-out value (TOV) for Modified Managed Fabric Name Monitoring (M-MFNM) mode.

Synopsis **timeout fnm** *value*

Operands *value* A value from 30 to 120 seconds.

Defaults The default is 120 seconds

Command Modes Access Gateway configuration mode

Description You must be in Access Gateway (AG) configuration mode to use this command. Use this command to set the time out value (TOV) for M-MFNM queries of the fabric name to detect whether all N_Ports in a port group are physically connected to the same physical or virtual fabric. M-MFNM is a Port Grouping mode that prevents connections from the AG VDX switch to multiple SANs.

Usage Guidelines Entering the **timeout fnm** command without a value displays the current TOV value.

Examples Set the fabric name monitoring TOV value.

```
sw0(config-rbridge-id-3-ag)# timeout fnm 60
```

Displays the fabric name monitoring TOV value.

```
sw0(config-rbridge-id-3-ag)# timeout fnm
```

See Also None

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 at which OSPF LSAs are collected into a group and refreshed, check-summed, or aged by the OSPF process. Valid values range from 10 to 1800 seconds. The default is 240 seconds.

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. Valid values range from 0 to 60000 milliseconds. The default is 0 milliseconds.

hold Minimum hold time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 5000 milliseconds.

max Maximum wait time between two consecutive SPF calculations. Valid values range from 0 to 60000 milliseconds. The default is 10000 milliseconds.

Defaults Refer to the Operands for specific defaults.

Command Modes OSPF VRF router configuration mode

Description Use this command to configure LSA pacing and SPF throttle timers.

Usage Guidelines 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.

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.

Enter the **no timers lsa-group-pacing** to restore the pacing interval to its default value.

Enter **no timers throttle spf** to set the SPF timers back to their defaults.

Examples To set the LSA group pacing interval to 30 seconds:

```
switch# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# router ospf
switch(config-router-ospf-vrf-default-vrf)# 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# configure
switch(config)# rbridge-id 5
switch(config-rbridge-id-5)# router ospf
switch(config-router-ospf-vrf-default-vrf)# timers throttle spf 10000 15000 30000
```

See Also None

timers (BGP)

Adjusts the interval at which BGP KEEPALIVE and HOLDTIME messages are sent.

Synopsis **timers** {**keep-alive** *keepalive_interval* **hold-time** *holdtime_interval*}
no timers

Operands **keep-alive** Sets the interval for KEEPALIVE messages.
 keepalive_interval
 The KEEPALIVE interval in seconds. Range is from 0 through 65535.
 Default is 60.

hold-time Sets the interval for HOLDTIME messages.
 holdtime_interval
 The HOLDTIME interval in seconds. Range is from 0 through 65535.
 Default is 180.

Defaults See Operands.

Command Modes BGP configuration mode

Description Use this command to adjust the interval at which BGP KEEPALIVE and HOLDTIME messages are sent.

Usage Guidelines The KEEPALIVE and HOLDTIME message interval is overwritten when the **fast-external-failover** command takes effect on a down link to a peer.

 You must enter a value for **keep-alive** before you can enter a value for **hold-time**. Both values must be entered.

 Use the **no timers** command to clear the timers.

Examples switch(config)# **rbridge-id 10**
 switch(config-rbridge-id-10)# **router bgp**
 switch(config-bgp-router)# **timers keep-alive 120 hold-time 360**

See Also **fast-external-failover (BGP)**

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*] [**vrf** *vrf-name*]

Operands

<i>dest-addr</i>	Specifies the IPv4 address of the destination device.
src-addr <i>address</i>	Specifies the IPv4 address of the source device.
ipv6 <i>dest-ipv6-addr</i>	Specifies the IPv6 address of the destination device. This parameter is valid only with the ping command.
maxttl <i>value</i>	Maximum Time To Live value in a number of hops.
minttl <i>value</i>	Minimum Time To Live value in a number of hops.
timeout <i>seconds</i>	The traceroute timeout value.
vrf <i>vrf-name</i>	When VRF is enabled, traceroute is available as a debugging tool.

Defaults None

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**

2

track

Specifies a VRRP 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	<i>rbridge-id/slot/port</i> Specifies a valid 40-gigabit Ethernet interface.
	<i>rbridge-id</i> Specifies the RBridge ID.
	<i>slot</i> Specifies a valid slot number.
	<i>port</i> Specifies a valid port number.
gigabitethernet	Specifies a valid 1-gigabit Ethernet interface
	<i>rbridge-id</i> Specifies the RBridge ID.
	<i>slot</i> Specifies a valid slot number.
	<i>port</i> Specifies a valid port number.
port-channel	<i>number</i> Specifies the port-channel number. Valid values range from 1 through 6144.
tengigabitethernet	Specifies a valid 10-gigabit Ethernet interface.
	<i>rbridge-id</i> Specifies the RBridge ID.
	<i>slot</i> Specifies a valid slot number.
	<i>port</i> Specifies a valid port number.
priority	<i>range</i> The track priority is a number from 1 through 254, and is used 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.

Defaults Priority range is 2.

Command Modes	Virtual-router-group configuration mode

Description	Use this command to specify a VRRP interface to track.

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

For VRRP, the tracked interface can be any 10-gigabit Ethernet, 40-gigabit Ethernet, 1-gigabit Ethernet, 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.

Enter **no track** with the specified interface to remove the tracked port configuration.

2 track

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(config-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 number of BPDUs than can be sent before pausing for 1 second. Valid unit values range from 1 through 10.

Defaults 6 units

Command Modes Protocol Spanning Tree MSTP configuration mode

Description Use this command to configure the BPDU burst size by changing the transmit hold count value.

Usage Guidelines Brocade Network OS v4.1.0 supports PVST+ and R-PVST+only. The PVST and R-PVST protocols are proprietary to Cisco and are not supported.
Enter **no transmit-holdcount** to return to the default setting.

Examples To change the number of BPDUs transmitted to 3 units:
`switch(config-mstp) # transmit-holdcount 3`

See Also **show spanning-tree mst detail**

transport-service

In a Virtual Fabrics context, associates a service VF with a trunk port interface as a transport VF.

Synopsis **transport-service** *tlsid*
 no transport-service *tlsid*

Operands *tlsid* The transport LAN service ID. Range is from 1 through 1000.

Defaults This feature is disabled by default.

Command Modes VLAN configuration mode

Description In a Virtual Fabrics context, use this command to associate a service VF (VLAN ID > 4095, through 8191) to a trunk port interface as a transport VF.

Usage Guidelines This command does not apply to standard (802.1Q) VLANs (VLAN IDs from 1 through 4095).
 This command is not supported when issued from a secondary node.
 Enter **no transport-service** *tlsid* to remove the service VF from the trunk port interface as a transport VF.

Examples Configure a classified VLAN and assign it to transport VF instance 10:

```
switch(config)# interface vlan 5000  
switch(config-vlan-5000)# transport-service 10
```

See Also interface vlan, vcs virtual-fabric enable

trunk-enable

Enables trunking on a Fibre Channel port.

Synopsis **trunk-enable**
 no trunk-enable

Operands None

Defaults Trunking is disabled.

Command Modes Interface Fibre Channel configuration mode

Description Use this command to enable 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.

Enter **no trunk-enable** to disable trunking on a Fibre Channel port.

Examples To enable trunking mode on a Fibre Channel port:

```
switch (config)# interface FibreChannel 7/0/2  
switch(config-FibreChannel-7/0/2)# trunk-enable
```

To disable trunking mode on a Fibre Channel port:

```
switch (config)# interface FibreChannel 7/0/2  
switch(config-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

udd enable

Enables the Unidirectional Link Detection (UDLD) protocol on an interface.

Synopsis **udd enable**
 no udd enable

Operands None

Defaults Disabled on interfaces by default.

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

Description Enables the UDLD protocol on the interface.

Usage Guidelines Use **no udd enable** to unblock the interface if it has been blocked by the UDLD protocol.

Examples To enable UDLD on a specific tengigabitethernet interface:

```
switch# configure  
switch(config)# interface te 5/0/1  
switch(conf-if-te-5/0/1)# udd enable
```

See Also **protocol udd**

unhide fips

Makes available irreversible commands used in enabling Federal Information Processing Standard (FIPS) compliance.

Synopsis **unhide fips**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Irreversible commands related to enabling FIPS compliance are hidden. Use this command to make the following hidden commands available: **fips root disable**, **fips selftests**, **fips selftests**, and **prom-access disable**.

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 used 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* [**rbridge-id** {*rbridge-id* | **all**}]

Operands	<i>name</i>	The name of the user account.
	rbridge-id	Enables RBridge ID mode to support VCS on individual nodes.
	<i>rbridge-id</i>	Specifies a unique identifier for a node.
	all	Specifies all identifiers for a node.

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 retries 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 sfp, username, unlock username**

update-time (BGP)

Configures the interval at which BGP next-hop tables are modified.

Synopsis **update-time** sec
 no update-time sec

Operands sec Update time in seconds. Range is from 0 through 30. Default is 5 seconds.

Defaults This option is disabled.

Command Modes BGP address-family IPv4 unicast configuration mode

Description Use this command to configure the interval at which BGP next-hop tables are modified. BGP next-hop tables should always have IGP (non-BGP) routes.

Usage Guidelines The update time determines how often the device computes the routes (next-hops) in an RBridge. Lowering the value set by the **update-time** command increases the convergence rate.

By default, the device updates the BGP4 next-hop tables and affected BGP4 routes five seconds following IGP route changes. Setting the update time value to 0 permits fast BGP4 convergence for situations such as a link failure or IGP route changes, starting the BGP4 route calculation in sub-second time.

Use the **no** form of this command to restore the defaults.

NOTE

Use the **advertisement-interval** command to determine how often to advertise IGP routes to the BGP neighbor.

Examples To permit fast convergence:

```
switch(config)# rbridge-id 10
switch(config-rbridge-id-10)# router bgp
switch(config-bgp-router)# address-family ipv4 unicast
switch(config-bgp-ipv4u)# update-time 0
```

See Also **advertisement-interval**

usb

Enables or disables an attached USB device.

Synopsis **usb {on | off}**

Operands **on** Turns the USB device on.
 off Turns the USB device off.

Defaults None

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 This command is executed on the local switch. 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**

Operands None

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to list the contents of an attached USB device.

Usage Guidelines This command is executed on the local switch. 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*

Operands **directory** *directory* Specifies one the name of the directory where the file you want to remove is located. Valid USBstorage directories are /firmware, /firmwarekey, /support, and /config.

file *file* Specifies the name of the file to be removed.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to remove a directory or a file from an attached USB device.

Usage Guidelines This command is executed on the local switch. 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**

user (alias configuration)

Launches the user level alias configuration mode.

Synopsis **user** *string*
 no user *string*

Operands *string* Alias name string. The number of characters can be from 1 through 64.

Defaults None

Command Modes Alias configuration mode

Description Use this command to launch the user-level alias configuration mode. This name is only visible to the user currently logged in to the switch. Use the **alias** command to configure the alias for the user name.

Use the **no** form of this command to remove the user.

Usage Guidelines None

Examples Example of setting a switch alias and a user alias.

```
switch(config)# alias-config  
switch(config-alias-config)# alias redwood engineering  
switch(config-alias-config)# user john  
switch(config-alias-config-user)# alias johnexpansion smith  
switch(config-alias-config-user)# alias userinfo show users
```

See Also **alias, alias-config**

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 <i>password</i>	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 <i>role_name</i>	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 <i>description</i>	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.

**CAUTION**

All active login sessions for a user are terminated if the user's password or role is changed.

Usage Guidelines The *username* must be between 1 and 16 alphanumeric characters in length.
 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.
 Enter **no username** *name* followed by the appropriate parameter name to set the individual parameters to their default values.

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**

username admin enable false

Toggles the lockout option for the default admin account.

Synopsis	username admin enable false no username admin enable false
Operands	None
Defaults	This feature is disabled.
Command Modes	Global configuration mode
Description	This command toggles the lockout option for the default admin account. The account lockout policy locks an account when the user exceeds the configured number of maximum failed login attempts. This policy is now available for admin accounts. You are allowed to enable or disable lockout policy for admin accounts and user accounts with the admin role. For admin accounts, there is no support of lockout duration to release the locked accounts. Locked admin role accounts will be reset after reboot.
Usage Guidelines	Use the no username admin enable false command to disable this option.
Examples	None
See Also	None

username user enable false

Toggles the lockout option for user accounts with admin privileges.

Synopsis **username user enable false**
 no username user enable false

Operands None

Defaults This feature is disabled.

Command Modes Global configuration mode

Description This command toggles the enable option for user accounts with admin privileges.

The account lockout policy locks an account when the user exceeds the configured number of maximum failed login attempts. This policy is now available for admin accounts. You are allowed to enable or disable lockout policy for admin accounts and user accounts with 'admin' role.

Usage Guidelines Use the **no username user enable false** command to disable this option.

Examples None

See Also None

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 **vc-link-init** is **idle**.

Command Modes Interface Fibre Channel configuration mode

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

Authenticates with an established vCenter and provides additional options.

Synopsis **vcenter** *name* [**activate** | **interval** *interval* | {**url** *URL* **username** *username* **password** *password*}]
no vcenter *name*

Operands

<i>name</i>	Name of an established vCenter.
activate	Activates the vCenter.
interval	Enables the discovery timer.
<i>interval</i>	Discovery timer interval in minutes, Range is 0 through 1440. Default is 30, and 0 disables discovery.
url	Enables configuration of vCenter URL, user name, and password.
<i>URL</i>	URL of the vCenter.
username	Configures the user name.
password	Configures the password.

Defaults None

Command Modes Global configuration mode

Description You must authenticate with an established vCenter before you can initiate any discovery transactions. In order to authenticate with a specific vCenter, you must configure the URL, login, and password properties on the VDX switch. Use this command to authenticate with a vCenter; establish a URL, username, and password; and manage discovery intervals.

Usage Guidelines Enter **no vcenter** *name* and selected operands to deactivate this functionality.

Example

```
switch(config)# vcenter myvcenter url https://10.2.2.2 username user
password pass
switch(config)# vcenter myvcenter activate
switch(config)# no vcenter myvcenter activate
switch(config)# no vcenter myvcenter
switch(config)# vcenter myvcenter interval 60
```

See Also **show vlan private-vlan**

vcenter discovery (ignore delete responses)

Causes a vCenter to ignore delete responses.

Synopsis **vcenter** *name* **discovery ignore-delete-all-response** [*number* | **always**]

Operands

<i>name</i>	Name of the vcenter.
<i>number</i>	Number of discovery cycles to ignore. Default is 0.
always	Always ignore delete-all requests from the vCenter.

Defaults The default for *number* is 0.

Command Modes Global configuration mode

Description An invalid state or condition of a vCenter can cause the deletion of all auto-port-profiles in a system. To prevent this from happening, you can configure a mode in Network OS to ignore the “delete-all” responses from the vCenter.

Usage Guidelines None

Examples `switch(config)# vcenter vcs_demo discovery ignore-delete-all-response 3`

See Also None

vcs (logical chassis cluster mode)

Changes RBridge ID and/or VCS ID of a logical chassis cluster mode and, with the **no** form of the command, converts a logical chassis cluster to a fabric cluster.

Synopsis	vcs [rbridge-id <i>rbridge-id</i>] [vcsid <i>vcsid</i>] no vcs [rbridge-id <i>rbridge-id</i>] [vcsid <i>vcsid</i>] logical-chassis enable no vcs logical-chassis enable rbridge-id {all <i>range</i>} default-config
Operands	rbridge-id <i>rbridge-id</i> Changes the existing RBridge ID. vcsid <i>vcsid</i> Changes the VCS ID. The range for this value is 1 to 8192. The default is 1. logical-chassis enable Used with the no form of this command, transitions the node from logical chassis cluster mode to fabric cluster mode. rbridge-id {all <i>range</i>} Specifies that you want to either convert all RBridge IDs in the logical chassis cluster to fabric cluster mode, or that you want to convert only a range of RBridge IDs. (You can also specify just one RBridge ID.) Ranges can be specified with hyphens, separated by commas, or contain a mixture of both. Do not use a space after a comma when specifying a range of IDs. For example, to specify RBridges 5 through 10 and RBridge 15, enter: rbridge-id 5,10,15 default-config Uses the default configuration when the nodes are converted to fabric cluster mode. This is a required parameter.
Defaults	None
Command Modes	Privileged EXEC mode
Description	Use this command to change the RBridge ID and/or the VCS ID on a switch. At the same time, you can change the VCS ID and transition the node from logical chassis cluster mode to fabric cluster mode. You can also convert the cluster from logical chassis cluster mode to fabric cluster mode without changing the RBridge ID or VCS ID.
Usage Guidelines	For examples of how to use the no form of this command, refer to the Examples.
Examples	To change the RBridge ID to 10 and VCS ID to 35: <pre>switch# vcs rbridge-id 10 vcsid 35</pre> To change an RBridge ID from 8 to 10: <pre>switch# vcs rbridge-id 10</pre> During reboot, enter the following command on the principal node to disable the old RBridge ID: <pre>switch# no vcs enable rbridge-id 8</pre>

2 vcs (logical chassis cluster mode)

The following provides examples of using the **no** form of this command.

Examples of using the "no" form of this command

Command	Command Behavior
switch# no vcs rbridge-id <x> logical chassis enable	Changes the RBridge ID of the node to the value <x> and then transitions the node from logical chassis cluster mode to fabric cluster mode.
switch# no vcs vcs-id <y> logical chassis enable	Changes the VCS ID of the node to the value <y> and then transitions the node from logical chassis cluster mode to fabric cluster mode.
no vcs rbridge-id <x> vcsid <y> logical chassis enable	Changes the RBridge ID of the node to the value <x>, changes the VCS ID of the node to the value <y>, and then transitions the node from logical chassis cluster mode to fabric cluster mode.
no vcs logical-chassis enable rbridge-id all default-config	Converts the entire logical chassis cluster (all RBridge IDs) to fabric cluster mode. The nodes will then use the default configurations for fabric cluster mode.
no vcs logical-chassis enable rbridge-id 1,4-8 default-config	Converts RBridge IDs 1 and 4 through 8 from logical chassis cluster mode to fabric cluster mode. These RBridge IDs will then use the default configurations for fabric cluster mode.

See Also vcs (standalone mode), vcs logical-chassis enable (fabric cluster mode), vcs rbridge-id (fabric cluster mode), vcs vcsid (fabric cluster mode), vcs virtual ip, vcs config snapshot (logical chassis cluster mode)

vcs (standalone mode)

Configures Brocade VCS Fabric technology parameters and can enable one of the two types of Brocade VCS fabric modes: *fabric cluster mode* or *logical chassis cluster mode*.

NOTE

Platforms that allow standalone mode are the Brocade VDS 6710-54, 6720, and 6730.

Synopsis	vcs [[rbridge-id rbridge-id] [vcsld ID] [enable]] vcs [[rbridge-id rbridge-id] [vcsld ID] [logical-chassis enable]] no vcs enable no logical-chassis 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. vcsld ID Sets the VCS ID. This parameter cannot be configured in standalone mode unless the enabling operation is performed at the same time. enable Enables Brocade VCS fabric cluster mode. logical-chassis enable Enables Brocade VCS logical chassis cluster 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 either of the two types of Brocade VCS fabric modes: <i>fabric cluster mode</i> or <i>logical chassis cluster mode</i> . You can set the Brocade VCS Fabric parameters and enable one of the VCS modes at the same time, or you can enable one of the VCS modes and then perform the ID assignments separately.
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 commands shown in the "Synopsis" section above. You can use the no form of this command as follows: - To transition a switch from either fabric cluster mode or logical chassis cluster mode back to standalone mode, run the command: no vcs enable - To transition a switch from logical chassis cluster mode back to fabric cluster mode, run the command: no logical-chassis enable
Examples	The following provides command examples of enabling Brocade VCS logical chassis cluster mode:

Command examples for enabling logical chassis cluster mode

Command	Command Behavior
switch# vcs logical-chassis enable	The VCS ID becomes the default value of 1, the RBridge ID is not changed, and Brocade VCS logical chassis cluster mode is enabled.
switch# vcs vcsid 22 rbridge-id 15 logical-chassis enable	The VCS ID is changed to 22, the RBridge ID is changed to 15, and Brocade VCS logical chassis cluster mode is enabled.
switch# vcs vcsid 11 logical-chassis enable	The VCS ID is changed to 11, the RBridge ID is not changed, and Brocade VCS logical chassis cluster mode is enabled.
switch# vcs rbridge-id 6 logical-chassis enable	The VCS ID becomes the default value of 1, the RBridge ID is changed to 6, and Brocade VCS logical chassis cluster mode is enabled.

The following provides command examples of enabling Brocade VCS fabric cluster mode:

Command examples for enabling fabric cluster mode

Command	Command Behavior
switch# vcs enable	The VCS ID becomes 1, the RBridge ID is not changed, and Brocade VCS fabric cluster mode is enabled.
switch# vcs vcsid 55 rbridge-id 19 enable	The VCS ID is changed to 55, the RBridge ID is changed to 19, and Brocade VCS fabric cluster mode is enabled.
switch# vcs vcsid 73 enable	The VCS ID is changed to the value of 73, the RBridge ID is not changed, and Brocade VCS fabric cluster mode is enabled.
switch# vcs rbridge-id 10 enable	The VCS ID becomes the default value 1, the RBridge ID is changed to 10, and Brocade VCS fabric cluster mode is enabled.

The following provides command examples for switches that are already in either fabric cluster mode or logical chassis cluster mode.

Command examples when one of the VCS modes is already enabled:

Command	Command Behavior
vcs vcsid 44 rbridge-id 22	The VCS ID is changed to 44 and the RBridge ID is changed to 22.
vcs vcsid 34	The VCS ID is changed to 34.

See aSo **vcs logical-chassis enable (fabric cluster mode), vcs rbridge-id (fabric cluster mode), vcs vcsid (fabric cluster mode), vcs (logical chassis cluster mode), vcs config snapshot (logical chassis cluster mode)**

vcs config snapshot (logical chassis cluster mode)

Takes a configuration snapshot for a specified RBridge ID.

Synopsis **vcs config snapshot {create | restore} rbridge-id *rbridge-id* snapshot-id *snapshot-id***
no vcs config snapshot rbridge-id *rbridge-id* snapshot-id [all | *rbridge-id*]

Operands

create	Captures the snapshot configuration from the RBridge ID specified.
restore	Restores the snapshot configuration to the RBridge ID specified.
rbridge-id <i>rbridge-id</i>	RBridge ID of the configuration you are capturing in a snapshot or the RBridge ID to which you are restoring the snapshot.
snapshot-id <i>snapshot-id</i>	Name you give to the snapshot of the configuration.
all	Designates all of the snapshots.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to take a configuration snapshot for an RBridge ID in a logical chassis cluster so that this configuration can be restored later if necessary. The snapshot for the RBridge specified is stored on all switches in the logical chassis cluster.

Usage Guidelines The **vcs config snapshot** commands apply onto to nodes in a logical chassis cluster mode. The **create** and **restore** commands can be issued from any node in the cluster even though the commands pertain to a specific RBridge ID.

If a snapshot was taken on a node that had been disconnected from the cluster, the cluster will not have the snapshot. In this situation, you can use the **copy snapshot** commands to put the snapshot on the cluster. Refer to “copy snapshot (logical chassis cluster mode)” on page 1674.

Create and restore commands can only be issued from the primary node and not from any other node.

Examples To create a snapshot of the configuration on an RBridge with the ID of 10, and to give the name of the snapshot "snapshot10:"

```
switch# vcs config snapshot create rbridge-id 10 snapshot snapshot10
```

See Also **vcs (standalone mode)**, **vcs logical-chassis enable (fabric cluster mode)**, **vcs rbridge-id (fabric cluster mode)**, **vcs vcsid (fabric cluster mode)**, **vcs (logical chassis cluster mode)**, **vcs virtual ip**,

vcs logical-chassis enable (fabric cluster mode)

Changes specified nodes from fabric cluster mode to logical chassis cluster mode.

Synopsis **vcs logical-chassis enable rbridge-id {all | range} default-config**
no vcs logical-chassis enable rbridge-id {all | range} default-config

Operands **rbridge-id [all | range]** Specifies that you want to either convert all RBridge IDs in the fabric cluster from fabric cluster mode to logical chassis mode, or that you want to convert only a range of RBridge IDs. (You can also specify just one RBridge ID.) Ranges can be specified with hyphens, separated by commas, or contain a mixture of both. Do not use a space after a comma when specifying a range of IDs. For example, to specify RBridges 5 through 10 and RBridge 15, enter: **rbridge-id 5,10,15**

default-config Uses the default configuration when the nodes are converted to logical chassis mode. This is a required parameter.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to change specified nodes from fabric cluster mode to logical chassis mode. In logical chassis mode, configuration can be distributed from one node—the primary switch—to all other nodes in the cluster.

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 commands shown in the Synopsis.

This command can be run only when the switch is in fabric cluster mode. All nodes you want to convert to logical chassis cluster mode must have the same global configuration for this command to work.

Conversely, the **no** form of the command can be run only when the switch is in logical chassis cluster mode and you want to convert it to fabric cluster mode.

Examples To convert all RBridge IDs in the fabric cluster to logical chassis cluster mode:

```
switch# vcs logical-chassis enable rbridge-id all default-config
```

See Also **vcs (standalone mode), vcs rbridge-id (fabric cluster mode), vcs vcsid (fabric cluster mode), vcs (logical chassis cluster mode), vcs virtual ip, vcs config snapshot (logical chassis cluster mode)**

vcs rbridge-id (fabric cluster mode)

Changes the RBridge ID and, optionally, the VCS ID, and can enable logical chassis cluster mode.

Synopsis `vcs rbridge-id rbridge-id [logical-chassis enable | vcsid vcsid [logical-chassis enable]]`

Operands `rbridge-id rbridge-id` Allows you to change the existing RBridge ID, and gives you the option of changing the VCS ID at the same time. While changing these IDs, you can also enable logical chassis cluster mode on the specified RBridge ID.

`vcsid vcsid` Changes the VCS ID. The range for this value is 1 to 8192. The default is 1.

`logical-chassis enable` Enables logical chassis cluster mode on the switch.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to change the RBridge ID on a switch. At the same time, you can change the VCS ID and enable the logical chassis cluster mode for the switch.

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 commands shown in the Synopsis.

To transition a switch from logical chassis cluster mode back to standalone mode, run the command: **no vcs enable**

NOTE

Platforms that allow standalone mode are the Brocade VDS 6710-54, 6720, and 6730.

Examples To convert a node that is in fabric cluster mode to logical chassis cluster mode, while simultaneously changing its RBridge ID to 10 and its VCS ID to 35:

```
switch# vcs rbridge-id 10 vcsid 35 logical-chassis enable
```

See Also `vcs (standalone mode)`, `vcs logical-chassis enable (fabric cluster mode)`, `vcs vcsid (fabric cluster mode)`, `vcs (logical chassis cluster mode)`, `vcs virtual ip`, `vcs config snapshot (logical chassis cluster mode)`

vcs vcsid (fabric cluster mode)

Changes the VCS ID and, optionally, the RBridge ID, and can enable logical chassis cluster mode.

Synopsis	vcs vcsid <i>vcsid</i> [logical-chassis enable rbridge-id <i>rbridge-id</i> [logical-chassis enable]]	
Operands	vcsid <i>vcsid</i>	Changes the existing VCS ID. The range for this value is 1 to 8192. The default is 1.
	rbridge-id <i>rbridge-id</i>	Changes the existing RBridge ID.
	logical-chassis enable	Enables logical chassis cluster mode on the switch.
Defaults	None	
Command Modes	Privileged EXEC mode	
Description	Use this command to change the VCS ID on a switch. At the same time, you can change the RBridge ID and enable the logical chassis cluster mode for the switch.	
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 commands shown in the Synopsis.	
	To transition a switch from logical chassis cluster mode back to standalone mode, run the command: no vcs enable	
	NOTE Platforms that allow standalone mode are the Brocade VDS 6710-54, 6720, and 6730.	
Examples	To convert a node that is in fabric cluster mode to logical chassis cluster mode, while simultaneously changing its RBridge ID to 10 and its VCS ID to 35: switch# vcs vcsid 35 rbridge-id 10 logical-chassis enable	
See Also	vcs (standalone mode), vcs logical-chassis enable (fabric cluster mode), vcs rbridge-id (fabric cluster mode), vcs (logical chassis cluster mode), vcs virtual ip , vcs config snapshot (logical chassis cluster mode)	

vcs virtual-fabric enable

Enables the Virtual Fabrics feature, allowing the configuration of service or transport VFs in a Virtual Fabrics context. This expands the VLAN ID address space above the standard 802.1Q limit of 4095 to support multitenancy.

Synopsis **vcs virtual-fabric enable**
 no vcs virtual-fabric enable

Operands None

Defaults This feature is disabled by default.

Command Modes Global configuration mode

Description Use this command to enable the configuration of service or transport VFs in a Virtual Fabrics context, with VLAN IDs above the standard 802.1Q limit of 4095 and through 8191. Refer to the Usage Guidelines.

Usage Guidelines This command will be successful only if the Virtual Fabric (VF) status is VF-capable. This operation does not disrupt existing 802.1Q traffic in the fabric. Upon the successful completion of the command, the status of the fabric becomes VF-enabled.

Use the **no** form of this command to disable the configuration of service or transport VFs in the fabric. The **no** form of this command will be successful only if there is no service or transport VF configuration in the fabric and the status of the fabric is VF-enabled. All service or transport VF configurations in the fabric must be removed or the command **no vcs virtual-fabric enable** will fail. Upon successful completion of the command, the fabric status becomes VF-capable.

On the Brocade VDX family of switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

NOTE

When the fabric is VF-enabled with a VF-specific configuration, the user is advised of relevant errors when attempting to disable the VF.

Examples To enable the Virtual Fabrics feature:

```
switch(config)# vcs virtual-fabric enable
```

To disable the Virtual Fabrics feature when there is no classified VLAN configuration in the fabric:

```
switch(config)# no vcs virtual-fabric enable
```

See Also interface vlan,

vcs replace rbridge-id

Replaces a node in a logical chassis cluster.

Synopsis `vcs replace rbridge-id rbridge-id`

Operands `rbridge-id rbridge-id` RBridge ID of the node you are replacing.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to replace a node in a logical chassis cluster with a new node. You need to re-use the RBridge ID and then enter the WWN of the new node when prompted, as shown in the Example.

Usage Guidelines This command can be performed only on a node that is in logical chassis cluster mode.

Examples To replace a node that has an RBridge ID of 3 and then enter the WWN of the new switch:

```
switch# vcs replace rbridge-id 3
Enter the WWN of the new replacement switch: 11:22:33:44:55:66:77:81
```

See Also None

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 by means of a CIDR prefix (mask).

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.

Usage Guidelines This command can be used in VCS 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.

Enter **no vcs virtual-ip address** to remove the currently-configured virtual IP address.

Examples To assign a virtual IP address and mask 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)# no vcs virtual ip address
```

See Also **show vcs**

virtual-fabric

Designates the FCoE Virtual Fabric Identification (VFID).

Synopsis	virtual-fabric 1
Operands	None
Defaults	None
Command Modes	FCoE fabric-map configuration mode
Description	Use this command to designate 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. NOTE The FCoE virtual fabric is not to be confused with the Virtual Fabric feature that supports service or transport VFs.
Examples	<pre>switch(config)# fcoe switch(config-fcoe)# fabric-map default switch(config-fcoe-fabric-map)# virtual-fabric 1</pre>
See Also	None

virtual-ip

Configures a virtual IPv4 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 IPv4 address of the virtual router.

Defaults None

Command Modes Virtual-router-group configuration mode

Description Use this command to configure a virtual IPv4 address for the virtual router.

This virtual IPv4 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.

Enter **no virtual-ip** *A.B.C.D* to delete the specified 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(config-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**

virtual-mac

Enables generation of a virtual MAC with 0 IP hash.

Synopsis `virtual-mac virtual_mac_address`

Operands `virtual_mac_address`

Defaults None

Command Modes VRRP-Extended group configuration mode

Description The distributed VXLAN gateway functionality depends on VRRP-E for multi-homing. By default, the VRRP-E virtual MAC is derived as 02:e0:52:<2-byte-ip-hash>:<1-byte-vrid>. The VXLAN gateway requires that the virtual MAC be a function of only VRID. The two-byte hash of the virtual IP should be set to 0s, as in the following example:

02e0.5200.00xx:<1-byte-VRID>

Usage Guidelines None

Examples To enable the generation of a virtual MAC with 0 IP hash:

```
switch(config)# rbridge-id 101
switch(config-rbridge-id-101)# int ve 10
switch(config-Ve-10)# vrrp-extended-group 100
switch(config-vrrp-extended-group-100)# virtual-mac 02e0.5200.00xx: <1-byte-VRID>
```

See Also

vlag ignore-split

Controls the ignore-split recovery functionality.

Synopsis **vlag ignore-split**
 no vlag ignore-split

Operands None

Defaults **vlag ignore-split** is enabled.

Command Modes Port-channel configuration mode

Description Use this command to enable or disable the ignore-split recovery functionality.

When ignore-split-recovery is active, neither of the R Bridges 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 supported only when the switch is operating in Brocade VCS Fabric mode.

Enter **no vlag ignore-split** to disable this functionality.

NOTE

It is recommended that this command be enabled.

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. Valid values range from 1 through 16.

vlan *vlan_id* Specifies which VLAN interface to activate. Refer to the Usage Guidelines.

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 switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

Enter **no vlan classifier activate group** *number* to remove the specified group.

Examples To activate VLAN classifier group 1 for VLAN 5 on a specific 10-gigabit Ethernet interface:

```
switch(config)# interface tengigabitethernet 178/0/1
switch(config-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

<i>number</i>	Specifies the VLAN group number for which rules are to be added or deleted. Valid values range from 1 through 16.
add rule <i>number</i>	Specifies a rule is to be added. Valid values range from 1 through 256.
delete rule <i>number</i>	Specifies a rule is to be deleted. Valid values range 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 switches, 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). Valid VLAN IDs are as follows:

- On Brocade VDX 8770 switches: 1 through 4086 for 802.1Q VLANs (VLAN IDs 4087 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.
- On all other Brocade VDX switches: 1 through 3962 for 802.1Q VLANs (VLAN IDs 3963 through 4095 are reserved on these switches), and 4096 through 8191 for service or transport VFs in a Virtual Fabrics context.

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	<i>rule_id</i>	Specifies the VLAN identification rule. Valid values range from 1 through 2556.
	mac	Specifies the Media Access Control (MAC) list.
	<i>mac_address</i>	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.
	<i>hex_addr</i>	An Ethernet hexadecimal value. Valid values range 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.

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.

Enter **no vlan classifier rule** *rule_id* to delete the specified rule.

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 802.1Q tagging on the native VLAN.

Synopsis **vlan dot1q tag native**
no vlan dot1q tag native

Operands None

Defaults The native VLAN is enabled.

Command Modes Global configuration mode

Description Use this command to enable dot1q (IEEE 802.1Q) tagging for all native VLANs on all trunked ports on the switch.

Usually, you configure 802.1Q trunks with a native VLAN ID, which strips tagging from all packets on that VLAN.

To maintain the tagging on the native VLAN and drop untagged traffic, use the **vlan dot1q tag native** command. The switch will tag the traffic received on the native VLAN and admit only 802.1Q-tagged frames.

Control traffic continues to be accepted as untagged on the native VLAN on a trunked port, even when the **vlan dot1q tag native** command is enabled.

Usage Guidelines Enter **no vlan dot1q tag native** to disable dot1q (IEEE 802.1Q) tagging for all native VLANs on all trunked ports on the switch.

Examples None

See Also **switchport mode, switchport trunk allowed vlan rspan-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 configuration mode

Description Use this command to activate the VLAN profile mode for AMPP. This mode allows configuration of VLAN attributes of a port-profile.

Usage Guidelines Enter **no vlan-profile** to delete the profile.

Examples To create a basic VLAN profile supporting 802.1Q VLANs:

```
switch(config)# port-profile my_profile
switch(conf-port-profile-my_profile)# vlan-profile
```

The following illustrates the creation of port-profiles and vlan-profiles with switchport configurations illustrating VLAN classifications in a Virtual Fabrics context:

```
sw0(config)# port-profile pp100
sw0(config-port-profile-pp100)# vlan-profile
sw0(config-vlan-profile)# switchport
sw0(config-vlan-profile)# switchport access vlan 5001 mac 1.1.1
sw0(config-vlan-profile)# switchport access vlan 5002 mac 1.1.2
sw0(config-vlan-profile)# switchport access vlan 5001 mac-group 11

sw0(config-vlan-profile)# port-profile pp101
sw0(config-port-profile-pp101)# vlan-profile
sw0(config-vlan-profile)# switchport
sw0(config-vlan-profile)# switchport mode trunk
sw0(config-vlan-profile)# switchport trunk allowed vlan add 5004 ctag 11
sw0(config-vlan-profile)# switchport trunk allowed vlan add 5005 ctag 12
sw0(config-vlan-profile)# switchport trunk native-vlan 5006 ctag 13
```

See Also None

vnetwork vcenter discover

Explicitly starts the discovery process on the vCenter.

Synopsis `vnetwork vcenter vcenter_name discover`

Operands `vcenter_name` Name of a vCenter.

Defaults None

Command Modes Privileged EXEC mode

Description Use this command to explicitly start the discovery process on the specified vCenter. 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 explicitly initiated with the CLI.

Usage Guidelines None

Examples None

See Also None

vrf

Creates and enters Virtual Routing and Forwarding (VRF) configuration mode.

Synopsis **vrf** *name*

Operands *name* Character string for the name of the VRF. The string can be up to 24 characters long, but should not contain punctuation or special characters.

Defaults None

Command Modes RBridge ID configuration mode

Description Use this command to create and enter Virtual Routing and Forwarding (VRF) configuration mode.

Usage Guidelines None

Examples None

See Also **address-family ipv4 unicast (BGP), arp, ip router-id, max-route, network (BGP), next-hop-recursion (BGP), rbridge-id, rd (route distinguisher)**

vrf-lite-capability (OSPF)

Disables the down-bit (DN bit) that is set when routes are redistributed from multiprotocol BGP (MP-BGP) to OSPF,

Synopsis **vrf-lite-capability**
 no vrf-lite-capability

Operands None

Defaults None

Command Modes OSPF VRF router configuration mode

Description Use this command to disable the down-bit (DN bit) that is set when routes are redistributed from multiprotocol BGP (MP-BGP) to OSPF. A customer edge (CE) router acts the provider edge (PE) router in VRF Lite. Because PE routers advertise VPN routes to CE routers with the DN-bit set, these checks should be disabled in a VRF Lite context. If CE routers receive routes with the DN-bit set, they discard those routes.

Usage Guidelines Enter **no vrf-lite-capability** to disable this feature.

Examples switch# **configure**
 switch(config)# **rbridge-id 5**
 switch(config-rbridge-id-5)# **router ospf vrf orange**
 switch(config-router-ospf-vrf-orange)# **vrf-lite-capability**

See Also None

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 user-assigned number from 1 through 128 that you assign to the virtual router group.

Defaults None

Command Modes Virtual Ethernet (ve) interface configuration mode

Description Use this command to identify a virtual-router-extended group and enter into the virtual router configuration mode.

Usage Guidelines This configuration is for virtual Ethernet (ve) interfaces only.

Enter **no vrrp-extended-group** *group-ID* to remove the 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-extended  
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 through 128 that you assign to the virtual router group.

Defaults None

Command Modes Interface subtype configuration mode

Description Use this command to identify a virtual router group and enters into the virtual router configuration mode.

Usage Guidelines Enter **no vrrp-group** *group-ID* 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 10-gigabit Ethernet 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 *aliasName*

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 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.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all R Bridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any R Bridge in a Brocade VCS Fabric, but it is always executed on the principal R Bridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal R Bridge.

Enter **member-entry** *member* [*; member*] ... 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.

Enter **no member-entry** *member* to remove a member from a zone alias. You can remove only one member entry each time you enter **no member-entry**.

If you remove the last member from a zone alias and subsequently commit the configuration, the commit operation deletes the zone alias.

Enter **no zoning defined-configuration alias** *aliasName* to delete a zone alias.

The **zoning defined-configuration alias** command changes the defined configuration.

To save the configuration persistently, enter **zoning enabled-configuration cfg-action cfg-save**. For the change to become effective, enable the configuration by entering **zoning enabled-configuration cfgName**.

Examples To create a zone alias with one member:

```
switch(config)# zoning defined-configuration alias alias1
```



```
switch(config-alias-alias1)# member-entry 10:00:00:00:00:00:01
```

To add two additional WWNs to the zone alias:

```
switch(config)# zoning defined-configuration alias alias1  
switch(config-alias-alias1)# member-entry \  
10:00:00:00:00:00:02;10:00:00:00:00:00:03
```

To remove a WWN from a zone alias:

```
switch(config)# zoning defined-configuration alias alias1  
switch(config-alias-alias1)# no member-entry 10:00:00:00:00:00:01
```

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 mode

Description Use this 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.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all R Bridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any R Bridge in a Brocade VCS Fabric, but it is always executed on the principal R Bridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal R Bridge.

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.

Enter **member-zone zoneName[;zoneName]...** 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.

Enter **no member-zone zoneName** 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.

Enter **no zoning defined-configuration cfg** *cfgName* to delete a configuration.

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.

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 cfg4
```

See Also zoning defined-configuration zone, zoning enabled-configuration cfg-name

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 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.

Usage Guidelines This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all R Bridges in the VCS Fabric. Standalone mode is not supported.

 This command can be entered on any R Bridge in a Brocade VCS Fabric, but it is always executed on the principal R Bridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal R Bridge.

 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.

 Enter **member-entry** *member* [*;* *member*] ... 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.

 Enter **no member-entry** *member* to remove a member from a zone. You can remove only one member entry each time you enter **no member-entry**.

 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.

 Enter **no zoning defined-configuration zone** *zoneName* 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.



CAUTION

For the change to become effective, enable the configuration with the **zoning enabled-configuration cfg-name** command. When edits are made to the defined configuration, and those edits affect a currently enabled zone configuration, issuing a “cfg-save” command makes the enabled configuration effectively stale. Until the enabled configuration is re-enabled, the merging of new RBridges into the cluster is not recommended. This merging may cause unpredictable results, with the potential for mismatched enabled-zoning configurations among the RBridges in the cluster.

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 zone3
```

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 defined zone information. The enabled configuration is not affected.
Usage Guidelines	This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all R Bridges in the VCS Fabric. Standalone mode is not supported. This command can be entered on any R Bridge in a Brocade VCS Fabric, but it is always executed on the principal R Bridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal R Bridge. After clearing the defined zone configuration with zoning enabled-configuration cfg-action cfg-clear, enter no zoning enabled-configuration cfg-name 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, enter zoning enabled-configuration cfg-action cfg-save to commit the transaction. If a cfg-clear is entered accidentally, issue a cfg-transaction-abort command.

**CAUTION**

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.

Examples	To clear the defined zoning database: <pre>switch(config)# zoning enabled-configuration cfg-action cfg-clear</pre>
See Also	zoning enabled-configuration cfg-name , 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 R Bridges in the VCS Fabric. Standalone mode is not supported. This command can be entered on any R Bridge in a Brocade VCS Fabric, but it is always executed on the principal R Bridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal R Bridge.
Examples	The following example saves the current zone configuration: <pre>switch(config)# zoning enabled-configuration cfg-action cfg-save</pre>
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 R Bridges in the VCS Fabric. Standalone mode is not supported. This command can be entered on any R Bridge in a Brocade VCS Fabric, but it is always executed on the principal R Bridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal R Bridge.
Examples	To abort the current zone transaction: <pre>switch(config)# zoning enabled-configuration cfg-action cfg-transaction-abort</pre>
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 Zoning is not implemented and default zoning applies.

Command Modes Global configuration mode

Description Use this command to enable a specific configuration. This command commits the current defined zone configuration to both volatile and nonvolatile memory.

Usage Guidelines Only one configuration can be enabled at a time.

This command is supported only in Brocade VCS Fabric mode. Zoning configuration data are automatically distributed among all R Bridges in the VCS Fabric. Standalone mode is not supported.

This command can be entered on any R Bridge in a Brocade VCS Fabric, but it is always executed on the principal R Bridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal R Bridge.

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.

Enter **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.

NOTE

If more than 300 devices are connected when the enabled-configuration is disabled, the **no zoning enabled-configuration cfg-name** command is not allowed if the defzone mode is AllAccess. In this case, change the defzone mode to No Access and then disable the enabled-configuration.

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	Zone access mode is “All Access”.	
Command Modes	Global configuration mode	
Description	Use this command to display or set 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 R Bridges in the VCS Fabric. Standalone mode is not supported.	
	This command can be entered on any R Bridge in a Brocade VCS Fabric, but it is always executed on the principal R Bridge in fabric cluster mode. In logical chassis cluster mode, edits can be performed only from the principal R Bridge.	
	ATTENTION 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 either the zoning enabled-configuration cfg-action cfg-save command or the zoning enabled-configuration cfg-name command.	
	NOTE A default zone controls the device access that 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.	
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-save	