Dell EMC Networking Command-Line Reference Guide for the C9010 Series

Version 9.14.1.5

DELL EMC

Notes, cautions, and warnings

NOTE: A NOTE indicates important information that helps you make better use of your product.

CAUTION: A CAUTION indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

WARNING: A WARNING indicates a potential for property damage, personal injury, or death.

© 2018 Dell Inc. or its subsidiaries. All rights reserved. Dell, EMC, and other trademarks are trademarks of Dell Inc. or its subsidiaries. Other trademarks may be trademarks of their respective owners.

2019 - 05

Rev. A01

Contents

1 About this Guide.....47
Objectives.....47
Audience.....47
Conventions.....47
Information Icons.....48

2 CLI Basics.....49
Accessing the Command Line.....49
Multiple Configuration Users.....49
Obtaining Help.....50
Navigating the CLI.....52
Using the Keyword no Command.....52
Filtering show Commands.....53
Command Modes.....54

3 Control and Monitoring.....64
asf-mode.....65
banner exec.....66
banner login.....67
banner motd.....69
cam-acl.....70
cam-audit linecard.....72
clear alarms.....73
clear average-power.....74
clear line.....74
configure.....75
debug cpu-traffic-stats.....76
debug ftpserver.....77
disable.....77
do.....78
enable.....79
enable cpu-clock-monitor.....80
enable optic-info-update interval.....81
end.....81
exec-timeout.....82
exit.....83
ftp-server enable.....84
ftp-server topdir.....85
ftp-server username.....86
hostname.....87
ip ftp password.....88
ip ftp source-interface.....89

ip ftp username....90
ip http source-interface....91
ip telnet server enable....92
ip telnet source-interface....93
ip tftp source-interface....94
line....95
logging coredump server....96
login concurrent-session....97
login statistics....99
ping....100
power on....103
reload....103
send....104
service timestamps....105
show alarms....107
show asf....109
show chassis....110
show command-history....111
show console lp....113
show cpu-traffic-stats....114
show cpu-interface-stats....115
show debugging....117
show environment....118
show inventory....120
show linecard....122
show login statistics....125
show memory....127
show processes cpu....129
show processes ipc....132
show processes ipc flow-control....136
show processes memory....139
show reset-reason....144
show rpm....146
show software ifm....148
show system linecard....149
show tech-support....150
show util-threshold cpu....162
show util-threshold memory....163
show version....164
telnet....167
terminal length....169
traceroute....170
undebug all....172
upload trace-log....172
util-threshold cpu....173

util-threshold memory....175
virtual-ip....176
write....177

4 File Management....179
boot system....179
cd....180
copy....182
delete....185
dir....186
format flash....188
mkdir....189
mount nfs....189
pwd....190
rename....191
restore factory-defaults....192
rmdir....193
show boot bmp....193
show boot system....194
show bootvar....195
show file....196
show file-systems....197
show os-version....199
show running-config....202
show startup-config....206
upgrade....207
upgrade system-image-os6....209
verify....210

5 802.1X....212
debug dot1x....213
dot1x auth-fail-vlan....214
dot1x auth-server....215
dot1x auth-type mab-only....215
dot1x authentication (Configuration)....216
dot1x authentication (Interface)....217
dot1x critical-vlan....218
dot1x guest-vlan....219
dot1x host-mode....220
dot1x mac-auth-bypass....221
dot1x max-eap-req....222
dot1x max-supplicants....223
dot1x port-control....223
dot1x profile....224
dot1x quiet-period....225
dot1x reauthentication....226

dot1x reauth-max....227
dot1x server-timeout....227
dot1x static-mab....229
dot1x supplicant-timeout....230
dot1x tx-period....231
mac....231
show dot1x cos-mapping interface....232
show dot1x interface....234
show dot1x profile....236

6 Access Control Lists (ACL)....238
Commands Common to all ACL Types....238
remark....239
show config....241
Common IP ACL Commands....241
clear counters ip access-group....242
ip access-group....242
ip control-plane egress-filter....244
show ip accounting access-list....245
Standard IP ACL Commands....246
deny....246
feature acloptimized....248
ip access-list standard....249
permit....250
resequence access-list....252
resequence prefix-list ipv4....253
seq....254
show ip access-lists....256
Extended IP ACL Commands....257
deny....257
deny icmp....259
deny tcp....262
deny udp....265
ip access-list extended....267
permit....269
permit icmp....271
permit tcp....272
permit udp....275
resequence prefix-list ipv4....278
seq....279
ACL VLAN Group Commands....282
acl-vlan-group....282
cam-acl-vlan....283
description (ACL VLAN Group)....284
ip access-group (ACL VLAN Group)....284
member vlan (ACL VLAN Group)....285

show acl-vlan-group 286
show cam-acl-vlan 287
show running config acl-vlan-group 288
Common MAC ACL Commands 289
clear counters mac access-group 289
mac control-plane egress-acl 290
mac access-group 290
show mac access-lists 292
show mac accounting access-list 293
Standard MAC ACL Commands 294
deny 294
mac access-list standard 296
permit 297
seq 299
Extended MAC ACL Commands 300
deny 300
mac access-list extended 302
permit 304
seq 306
IP Prefix List Commands 308
clear ip prefix-list 308
deny 309
ip prefix-list 310
permit 311
seq 312
show config 313
show ip prefix-list detail 314
show ip prefix-list summary 315
Route Map Commands 316
continue 316
description 317
match as-path 318
match community 319
match interface 320
match ip address 321
match ip next-hop 322
match ip route-source 323
match metric 324
match origin 325
match route-type 326
match tag 327
route-map 328
set as-path 329
set automatic-tag 330
set comm-list delete 331

set community....332
set level....333
set local-preference....334
set metric....335
set metric-type....336
set next-hop....337
set origin....338
set tag....339
set weight....340
show config....341
show route-map....341
AS-Path Commands....342
ip as-path access-list....342
show ip as-path-access-lists....343
IP Community List Commands....344
ip community-list....344
show ip community-lists....345

7 Bidirectional Forwarding Detection (BFD)....347
bfd all-neighbors....347
bfd disable....349
bfd enable (Configuration)....350
bfd enable (Interface)....350
bfd interval....351
bfd protocol-liveness....352
ip route bfd....353
ipv6 route bfd....354
ip ospf bfd all-neighbors....355
ipv6 ospf bfd all-neighbors....356
neighbor bfd....357
neighbor bfd disable....358
show bfd neighbors....359
vrrp bfd....361

8 Border Gateway Protocol....363
BGP IPv4 Commands....363
address-family....363
aggregate-address....364
bgp add-path....366
bgp always-compare-med....366
bgp asnotation....367
bgp bestpath as-path ignore....368
bgp bestpath as-path multipath-relax....369
bgp bestpath med confed....370
bgp bestpath med missing-as-best....370
bgp bestpath router-id ignore....371

bgp client-to-client reflection..... 372
bgp cluster-id.....372
bgp confederation identifier.....373
bgp confederation peers..... 374
bgp dampening.....375
bgp default local-preference.....377
bgp dmzlink-bw..... 377
bgp enforce-first-as.....378
bgp fast-external-fallover.....379
bgp four-octet-as-support..... 380
bgp graceful-restart..... 381
bgp log-neighbor-changes.....382
bgp non-deterministic-med..... 382
bgp outbound-optimization..... 383
bgp recursive-bgp-next-hop..... 384
bgp regex-eval-optz-disable.....385
bgp router-id.....386
bgp soft-reconfig-backup..... 387
capture bgp-pdu neighbor.....388
capture bgp-pdu max-buffer-size.....389
clear ip bgp..... 389
clear ip bgp dampening.....391
clear ip bgp flap-statistics.....392
clear ip bgp peer-group.....394
debug ip bgp.....395
debug ip bgp dampening..... 396
debug ip bgp events..... 397
debug ip bgp keepalives.....398
debug ip bgp notifications..... 399
debug ip bgp soft-reconfiguration.....400
debug ip bgp updates..... 401
default-metric.....402
deny bandwidth..... 403
description..... 404
distance bgp.....404
maximum-paths..... 405
neighbor activate..... 406
neighbor add-path..... 407
neighbor advertisement-interval.....408
neighbor advertisement-start..... 409
neighbor allowas-in.....409
neighbor default-originate..... 410
neighbor description..... 411
neighbor distribute-list..... 412
neighbor dmzlink-bw.....413

neighbor ebgp-multihop..... 414
neighbor fall-over..... 415
neighbor filter-list..... 416
neighbor local-as..... 417
neighbor maximum-prefix..... 418
neighbor next-hop-self..... 419
neighbor password..... 420
neighbor peer-group (assigning peers)..... 421
neighbor peer-group (creating group)..... 422
neighbor peer-group passive..... 423
neighbor remote-as..... 424
neighbor remove-private-as..... 425
neighbor route-map..... 426
neighbor route-reflector-client..... 427
neighbor send-community..... 428
neighbor shutdown..... 429
neighbor soft-reconfiguration inbound..... 430
neighbor subnet..... 431
neighbor timers..... 431
neighbor timers extended..... 432
neighbor update-source..... 433
neighbor weight..... 434
network..... 435
network backdoor..... 436
permit bandwidth..... 437
redistribute..... 438
redistribute ospf..... 439
router bgp..... 440
set extcommunity bandwidth..... 441
shutdown all..... 442
shutdown address-family-ipv4–multicast..... 442
shutdown address-family-ipv4–unicast..... 443
shutdown address-family-ipv6–unicast..... 443
show capture bgp-pdu neighbor..... 444
show config..... 445
show ip bgp..... 446
show ip bgp cluster-list..... 448
show ip bgp community..... 450
show ip bgp community-list..... 452
show ip bgp dampened-paths..... 454
show ip bgp detail..... 456
show ip bgp extcommunity-list..... 457
show ip bgp filter-list..... 459
show ip bgp flap-statistics..... 460
show ip bgp inconsistent-as..... 462

show ip bgp neighbors....464
show ip bgp next-hop....467
show ip bgp paths....468
show ip bgp paths as-path....470
show ip bgp paths community....471
show ip bgp peer-group....472
show ip bgp regexp....474
show ip bgp summary....475
show running-config bgp....478
timers bgp....479
timers bgp extended....480
MBGP Commands....480
debug ip bgp dampening....481
distance bgp....482
show ip bgp dampened-paths....483
BGP Extended Communities (RFC 4360)....484
deny....484
deny regex....485
description....486
ip extcommunity-list....487
match extcommunity....487
permit....488
permit regex....489
set extcommunity rt....490
set extcommunity soo....491
show ip bgp ipv4 extcommunity-list....492
show ip bgp paths extcommunity....493
show ip extcommunity-list....494
show running-config extcommunity-list....495
IPv6 BGP Commands....496
address-family....496
address family ipv6 unicast....496
aggregate-address....497
bgp always-compare-med....498
bgp bestpath as-path ignore....499
bgp bestpath med confed....499
bgp bestpath med missing-as-best....500
bgp client-to-client reflection....500
bgp cluster-id....501
bgp confederation identifier....502
bgp dampening....502
bgp default local-preference....503
bgp enforce-first-as....504
bgp fast-external-fallover....505
bgp four-octet-as-support....505

bgp graceful-restart 506
bgp log-neighbor-changes 507
bgp non-deterministic-med 507
bgp recursive-bgp-next-hop 508
bgp regex-eval-optz-disable 508
bgp router-id 509
bgp soft-reconfig-backup 510
capture bgp-pdu max-buffer-size 511
capture bgp-pdu neighbor (ipv6) 511
clear ip bgp ipv6-address 512
clear ip bgp * (asterisk) 513
clear ip bgp as-number 514
clear ip bgp ipv6 dampening 514
clear ip bgp ipv6 flap-statistics 515
clear ip bgp ipv6 unicast 516
clear ip bgp ipv6 unicast dampening 517
clear ip bgp ipv6 unicast flap-statistics 517
debug ip bgp keepalives 518
debug ip bgp ipv6 dampening 519
debug ip bgp ipv6 unicast peer-group updates 519
debug ip bgp ipv6 unicast dampening 520
debug ip bgp ipv6 unicast updates 520
debug ip bgp notifications 521
debug ip bgp updates 522
default-metric 522
description 523
distance bgp 524
ipv6 prefix-list 525
maximum-paths 525
neighbor activate 526
neighbor advertisement-interval 527
neighbor allowas-in 527
neighbor default-originate 528
neighbor description 529
neighbor distribute-list 530
neighbor ebgp-multihop 531
neighbor fall-over 531
neighbor filter-list 532
neighbor maximum-prefix 533
neighbor next-hop-self 534
neighbor peer-group (assigning peers) 534
neighbor peer-group (creating group) 536
neighbor peer-group passive 536
neighbor remote-as 537
neighbor remove-private-as 538

neighbor route-map....538
neighbor route-reflector-client....539
neighbor send-community....540
neighbor soft-reconfiguration inbound....541
neighbor subnet....542
neighbor shutdown....542
neighbor timers....543
neighbor update-source....544
neighbor weight....545
neighbor X:X:X::X password....545
network....546
network backdoor....547
redistribute....547
redistribute ospf....548
router bgp....549
show capture bgp-pdu neighbor....550
show config....550
show ip bgp next-hop....551
show ip bgp paths....552
show ip bgp paths as-path....552
show ip bgp paths community....553
show ip bgp paths extcommunity....553
show ip bgp regexp....554
show ipv6 prefix-list....555
show ip bgp ipv6 unicast....555
show ip bgp ipv6 unicast cluster-list....556
show ip bgp ipv6 unicast community....556
show ip bgp ipv6 unicast community-list....557
show ip bgp ipv6 unicast dampened-paths....558
show ip bgp ipv6 unicast detail....558
show ip bgp ipv6 unicast extcommunity-list....559
show ip bgp ipv6 unicast filter-list....559
show ip bgp ipv6 unicast flap-statistics....560
show ip bgp ipv6 unicast inconsistent-as....561
show ip bgp ipv6 unicast neighbors....561
show ip bgp ipv6 unicast peer-group....562
show ip bgp ipv6 unicast summary....563
timers bgp....564
IPv6 MBGP Commands....564
show ipv6 mbgproutes....565

9 Content Addressable Memory (CAM)....566
CAM Profile Commands....566
cam-acl (Configuration)....567
cam-acl-egress....569
cam-acl-egress-pe....570

cam-acl-pe ... 571
cam-optimization ... 572
cam-threshold ... 573
show cam-acl ... 574
show cam-usage ... 574
show cam-acl-pe ... 576
show cam-acl-egress-pe ... 577
test cam-usage ... 578
Unified Forwarding Table Modes ... 579
show hardware forwarding-table mode ... 579
hardware forwarding-table mode ... 580

10 Control Plane Policing (CoPP) ... 581
clear control-traffic protocol ... 581
clear control-traffic queue ... 582
control-plane-cpuqos ... 583
service-policy rate-limit-cpu-queues ... 584
service-policy rate-limit-protocols ... 584
show control-traffic protocol ... 585
show control-traffic queue ... 587
show cpu-queue rate ... 588
show ip protocol-queue-mapping ... 589
show ipv6 protocol-queue-mapping ... 590
show mac protocol-queue-mapping ... 591
show protocol-queue-mapping ... 592

11 Data Center Bridging (DCB) ... 596
DCB Commands ... 596
dcb-enable ... 597
PFC Commands ... 598
clear hardware pfc-nodrop-priority ... 598
clear pfc counters ... 598
dcb-input ... 599
dcb-policy input ... 600
dcb-policy input stack-unit stack-ports all ... 601
pfc no-drop queues ... 602
pfc-nodrop-priority l2-dlf drop ... 603
pfc priority ... 604
show dcb ... 605
show hardware pfc-nodrop-priority ... 605
show interface pfc ... 606
show interface pfc statistics ... 609
ETS Commands ... 611
dcb-enable ... 611
dcb-output ... 612
dcb-policy output ... 613

clear ets counters....613
show interfaces ets....614
DCBX Commands....620
advertise dcbx-tlv....621
dcbx port-role....622
dcbx version....623
debug dcbx....624
fcoe priority-bits....624
iscsi priority-bits....625
show interface dcbx detail....626
dcb-map....629
priority-pgid....630
priority-group bandwidth pfc....631
dcb-map stack-unit all stack-ports all....632
dcb pfc-shared-buffer-size....632
dcb-buffer-threshold....633
priority....634
qos-policy-buffer....635
dcb-policy buffer-threshold (Interface Configuration)....637
show qos dcb-buffer-threshold....637
show hardware stack-unit buffer-stats-snapshot....638
dcb pfc-total-buffer-size....645
show running-config dcb-buffer-threshold....646
dcb pfc-queues....648
dcb {ets | pfc} enable....649

12 Debugging and Diagnostics....650
Offline Diagnostic Commands....650
diag....650
offline linecard....652
offline system....653
show diag....654
show diag testcase....660
Hardware Commands....664
clear control-traffic....664
clear hardware....665
clear hardware system-flow....667
remote-exec....668
show hardware....669
show hardware buffer....682
show hardware ip....685
show hardware ipv6....687
show hardware mac....689
show hardware system-flow....691
tcpdump....693

13 Dynamic Host Configuration Protocol (DHCP)....695
Configure a DHCP Server and DHCP Clients....695
clear ip dhcp....695
debug ip dhcp client events....696
debug ip dhcp client packets....697
debug ip dhcp server....698
default-router....699
disable....700
dns-server....700
domain-name....701
excluded-address....701
hardware-address....702
host-address....703
ip address dhcp....703
ip address dhcp relay information-option....704
ip address dhcp vendor-class-identifier....705
ip dhcp relay secondary-subnet....706
ip dhcp server....706
ip helper-address....707
ipv6 helper-address....708
lease....709
netbios-name-server....710
netbios-node-type....710
network....711
pool....712
show ip dhcp client statistics....712
show ip dhcp configuration....713
show ip dhcp conflict....714
show ip dhcp lease....715
show ip dhcp server statistics....715
Configure Secure DHCP and DHCP Relay....716
arp inspection....716
arp inspection-trust....717
clear ip dhcp snooping....718
ip dhcp relay information-option....718
ip dhcp relay source-interface....719
ipv6 dhcp relay source-interface....720
ip dhcp snooping....721
ip dhcp snooping binding....722
ip dhcp snooping database....723
ip dhcp snooping database renew....724
ip dhcp snooping trust....724
ip dhcp snooping verify mac-address....725
ip dhcp snooping vlan....726
ip dhcp source-address-validation....726

show ip dhcp binding....727
show ip dhcp snooping....728

14 Equal Cost Multi-Path (ECMP)....730
ecmp-group....730
hash-algorithm ecmp....731
hash-algorithm hg....734
hash-algorithm hg-seed....735
hash-algorithm seed....735
ip ecmp-group....736
ip ecmp weighted....737
link-bundle-distribution trigger-threshold....738
link-bundle-monitor enable....738
show config....739
show link-bundle distribution....739

15 FCoE Transit....741
clear fip-snooping database interface vlan....741
clear fip-snooping statistics....742
debug fip snooping....743
debug fip snooping rx....743
feature fip-snooping....744
fip-snooping enable....745
fip-snooping fc-map....745
fip-snooping max-sessions-per-enodemac....746
fip-snooping port-mode fcf....747
fip-snooping port-mode fcoe-trusted....747
show fip-snooping config....748
show fip-snooping enode....749
show fip-snooping fcf....750
show fip-snooping sessions....751
show fip-snooping statistics....752
show fip-snooping system....755
show fip-snooping vlan....755

16 FIPS Cryptography....757
fips mode enable....757
show fips status....758
show ip ssh....758
ssh....759

17 Flex Hash and Optimized Boot-Up....763
encapsulation dot1q....763
lacp fast-switchover....764
load-balance flexhash....764
load-balance ingress-port enable....765

18 Force10 OS Resilient Ring Protocol (FRRP)....767
clear frrp....767
debug frrp....768
description....769
disable....770
interface....771
member-vlan....772
mode....773
protocol frrp....773
show frrp....774
timer....775

19 GARP VLAN Registration (GVRP)....777
clear gvrp statistics....778
debug gvrp....779
disable....780
garp timers....780
gvrp enable....782
gvrp registration....782
protocol gvrp....783
show config....784
show garp timers....785
show gvrp....785
show gvrp statistics....787

20 High Availability (HA)....789
redundancy auto-failover-limit....789
redundancy disable-auto-reboot....790
redundancy force-failover....791
redundancy primary....792
redundancy reset-counter....793
redundancy synchronize....793
show redundancy....794

21 ICMP Message Types....798

22 Interfaces....800
Basic Interface Commands....800
clear counters....800
clear dampening....803
combo-port-type....804
combo-port-type....805
dampening....805
description....807
default interface....808

encapsulation dot1q....809
flowcontrol....810
interface....812
interface loopback....814
interface ManagementEthernet....815
interface null....816
interface range....817
interface range macro (define)....820
interface range macro name....821
interface vlan....822
keepalive....823
linecard portmode....824
monitor interface....825
mtu....829
portmode hybrid....830
rate-interval....832
rate-interval (Configuration Mode)....833
show config....834
show config (from INTERFACE RANGE mode)....835
show interfaces....836
show interfaces configured....849
show interfaces dampening....852
show interfaces phy....856
show interfaces status....859
show interfaces switchport....864
show interfaces transceiver....868
show interfaces vlan....875
show range....876
show running-config ecmp-group....877
shutdown....877
speed (for 10/100/1000/10000 interfaces)....878
speed (Management interface)....880
switchport....881
wavelength....882
Egress Interface Selection (EIS) Commands....883
application....883
clear management application pkt-cntr....884
management egress-interface-selection....884
show ip management-eis-route....885
show management application pkt-cntr....885
show management application pkt-fallback-cntr....886
Port Channel Commands....887
channel-member....887
group....889
interface port-channel....890

minimum-links....891
port-channel failover-group....892
show config....893
show interfaces port-channel....894
show port-channel-flow....897
HiGig Port Channel Commands....899
clear hardware hg-stats....899
hg-link-bundle-monitor enable....901
hg-link-bundle-monitor rate-interval....901
hg-link-bundle-monitor trigger-threshold....902
show hardware hg-stats....903
show hg-link-bundle-distribution....905
snmp-server enable traps hg-lbm....906
Time Domain Reflectometer (TDR) Commands....906
tdr-cable-test....907
show tdr....908

23 Intermediate System to Intermediate System (IS-IS)....910
adjacency-check....912
advertise....913
area-password....914
clear isis....915
clns host....915
debug isis....916
debug isis adj-packets....917
debug isis graceful-restart....918
debug isis local-updates....919
debug isis snp-packets....920
debug isis spf-triggers....921
debug isis update-packets....921
default-information originate....922
description....924
distance....924
distribute-list in....925
distribute-list out....926
distribute-list redistributed-override....927
domain-password....928
graceful-restart ietf....929
graceful-restart interval....930
graceful-restart restart-wait....931
graceful-restart t1....931
graceful-restart t2....932
graceful-restart t3....933
hello padding....934
hostname dynamic....935
ignore-lsp-errors....936

ip router isis..... 936
ipv6 router isis..... 937
isis circuit-type..... 938
isis csnp-interval..... 939
isis hello-interval..... 940
isis hello-multiplier..... 941
isis hello padding..... 942
isis ipv6 metric..... 943
isis metric..... 944
isis network point-to-point..... 945
isis password..... 945
isis priority..... 946
is-type..... 947
log-adjacency-changes..... 948
lsp-gen-interval..... 949
lsp-mtu..... 950
lsp-refresh-interval..... 951
max-area-addresses..... 952
max-lsp-lifetime..... 953
maximum-paths..... 954
metric-style..... 955
multi-topology..... 956
net..... 956
passive-interface..... 957
redistribute..... 958
redistribute bgp..... 960
redistribute ospf..... 961
router isis..... 963
set-overload-bit..... 964
show config..... 965
show isis database..... 966
show isis graceful-restart detail..... 968
show isis hostname..... 970
show isis interface..... 970
show isis neighbors..... 973
show isis protocol..... 975
show isis traffic..... 976
spf-interval..... 978

24 Internet Group Management Protocol (IGMP)..... 980
IGMP Commands..... 980
clear ip igmp groups..... 980
debug ip igmp..... 981
ip igmp access-group..... 982
ip igmp group-join-limit..... 983
ip igmp immediate-leave..... 984

ip igmp last-member-query-interval....985
ip igmp querier-timeout....986
ip igmp query-interval....987
ip igmp query-max-resp-time....988
ip igmp ssm-map....989
ip igmp static-group....990
ip igmp version....991
show ip igmp groups....992
show ip igmp interface....994
show ip igmp ssm-map....995
IGMP Snooping Commands....996
clear ip igmp snooping groups....997
debug ip igmp snooping....997
ip igmp snooping enable....998
ip igmp snooping fast-leave....999
ip igmp snooping flood....1000
ip igmp snooping last-member-query-interval....1001
ip igmp snooping mrouter....1002
ip igmp snooping querier....1003
show ip igmp snooping mrouter....1004
show ip igmp snooping groups....1005

25 Internet Protocol Security (IPSec)....1007
crypto ipsec transform-set....1008
crypto ipsec policy....1009
management crypto-policy....1010
match....1010
session-key....1011
show crypto ipsec transform-set....1012
show crypto ipsec policy....1013
transform-set....1014

26 IPv4 Routing....1016
arp....1017
arp backoff-time....1018
arp learn-enable....1019
arp retries....1020
arp timeout....1021
clear arp-cache....1022
clear host....1023
clear ip fib linecard....1024
clear ip route....1024
clear ip traffic....1025
clear tcp statistics....1026
debug arp....1027
debug ip dhcp....1028

debug ip icmp..... 1029
debug ip packet..... 1031
deny arp (for Extended MAC ACLs)..... 1033
icmp6-redirect enable..... 1034
ip address..... 1035
ip directed-broadcast..... 1036
ip domain-list..... 1036
ip domain-lookup..... 1037
ip domain-name..... 1038
ip helper-address hop-count disable..... 1039
ip host..... 1040
ip max-frag-count..... 1041
ip name-server..... 1042
ip proxy-arp..... 1043
ip route..... 1043
ip source-route..... 1046
ip unreachables..... 1047
ipv4 unicast-host-route..... 1048
load-balance..... 1048
management route..... 1050
show arp..... 1051
show arp retries..... 1054
show hosts..... 1055
show ip cam linecard..... 1056
show ip fib linecard..... 1058
show ip flow..... 1059
show ip interface..... 1060
show ip management-route..... 1063
show ipv6 management-route..... 1064
show ip protocols..... 1065
show ip route..... 1066
show ip route list..... 1068
show ip route summary..... 1069
show ip traffic..... 1071
show tcp statistics..... 1073

27 IPv6 Access Control Lists (IPv6 ACLs)..... 1076
cam-acl..... 1077
cam-acl-egress..... 1079
clear counters ipv6 access-group..... 1081
deny (for IPv6 ACLs)..... 1081
deny icmp (for Extended IPv6 ACLs)..... 1083
deny tcp (for IPv6 ACLs)..... 1084
deny udp (for IPv6 ACLs)..... 1085
ipv6 access-list..... 1086
ipv6 control-plane egress-filter..... 1087

permit (for IPv6 ACLs)....1088
permit icmp (for IPv6 ACLs)....1089
permit tcp (for IPv6 ACLs)....1090
permit udp (for IPv6 ACLs)....1092
seq (for IPv6 ACLs)....1093
show cam-usage....1094
show ipv6 access-list....1096
show ipv6 accounting access-list....1097
show running-config....1098

28 IPv6 Basics....1100
cam-ipv6 extended-prefix....1101
clear ipv6 fib....1101
clear ipv6 mld_host....1102
clear ipv6 neighbors....1103
ipv6 address....1104
ipv6 address autoconfig....1105
ipv6 address eui64....1106
ipv6 control-plane icmp error-rate-limit....1107
ipv6 flowlabel-zero....1108
ipv6 host....1108
ipv6 name-server....1109
ipv6 nd dad attempts....1110
ipv6 nd disable-reachable-timer....1111
ipv6 nd dns-server....1111
ipv6 nd prefix....1112
ipv6 neighbor....1113
ipv6 route....1115
ipv6 unicast-host-route....1117
ipv6 unicast-routing....1118
show cam-ipv6 extended-prefix....1119
show ipv6 cam linecard....1119
show ipv6 control-plane icmp....1120
show ipv6 fib linecard....1121
show ipv6 flowlabel-zero....1122
show ipv6 interface....1123
show ipv6 mld_host....1126
show ipv6 neighbors....1127
show ipv6 route....1128

29 iSCSI Optimization....1132
advertise dcbx-app-tlv....1132
iscsi aging time....1133
iscsi cos....1133
iscsi enable....1134
iscsi priority-bits....1135

iscsi profile-compellant....1135
iscsi target port....1136
show iscsi....1136
show iscsi session....1137
show iscsi session detailed....1138
show run iscsi....1139

30 Layer 2....1140
MAC Addressing Commands....1140
clear mac-address-table....1140
mac-address-table aging-time....1141
mac-address-table disable-learning....1142
mac-address-table static....1143
mac-address-table station-move refresh-arp....1144
mac-address-table station-move threshold....1145
mac learning-limit....1146
mac learning-limit learn-limit-violation....1148
mac learning-limit mac-address-sticky....1148
mac learning-limit station-move-violation....1149
mac learning-limit reset....1150
mac port-security....1151
show cam mac linecard (dynamic or static)....1151
show mac-address-table....1153
show mac-address-table aging-time....1155
show mac learning-limit....1156
Virtual LAN (VLAN) Commands....1157
default vlan-id....1158
default-vlan disable....1159
name....1159
show config....1160
show vlan....1161
tagged....1164
track ip....1165
untagged....1166
Far-End Failure Detection (FEFD)....1167
debug fefd....1168
fefd....1169
fefd disable....1170
fefd interval....1170
fefd mode....1171
fefd reset....1172
fefd-global interval....1173
fefd-global....1173
show fefd....1174

31 Link Aggregation Control Protocol (LACP)....1177

clear lacp counters....1177
debug lacp....1178
lacp long-timeout....1179
lacp port-priority....1180
lacp system-priority....1181
port-channel mode....1181
port-channel-protocol lacp....1182
show lacp....1183

32 Link Layer Discovery Protocol (LLDP)....1185
LLPD Commands....1185
advertise dot1-tlv....1185
advertise dot3-tlv....1186
advertise interface-port-desc....1187
advertise dot3-tlv....1188
advertise management-tlv....1188
advertise management-tlv (Interface)....1189
clear lldp counters....1190
clear lldp neighbors....1191
debug lldp interface....1192
disable....1194
hello....1195
management-interface....1195
mode....1196
multiplier....1197
protocol lldp (Configuration)....1197
protocol lldp (Interface)....1198
show lldp neighbors....1199
show lldp statistics....1202
show management-interface....1203
show running-config lldp....1204
snmp-notification-interval....1204
LLDP-MED Commands....1205
advertise med guest-voice....1205
advertise med guest-voice-signaling....1206
advertise med location-identification....1207
advertise med power-via-mdi....1208
advertise med softphone-voice....1209
advertise med streaming-video....1210
advertise med video-conferencing....1211
advertise med video-signaling....1212
advertise med voice....1213
advertise med voice-signaling....1214

33 Multicast....1216
IPv4 Multicast Commands....1216

clear ip mroute....1216
mtrace....1217
ip mroute....1218
ip multicast-limit....1219
ip multicast-routing....1220
show ip multicast-cam....1221
show ip mroute....1222
show ip rpf....1224
IPv6 Multicast Commands....1225
clear ipv6 mroute....1225
ipv6 multicast-routing....1225
show ipv6 mroute....1226
show ipv6 multicast-cam....1227
show ipv6 rpf....1228

34 Multicast Listener Discovery Protocol....1229
clear ipv6 mld groups....1229
debug ipv6 mld....1230
ipv6 mld explicit-tracking....1230
ipv6 mld last-member-query-interval....1231
ipv6 mld query-interval....1231
ipv6 mld query-max-resp-time....1232
ipv6 mld version....1232
show ipv6 mld groups....1233
show ipv6 mld interface....1233
MLD Snooping....1234
clear ipv6 mld snooping groups....1234
debug ipv6 mld snooping....1235
ipv6 mld snooping....1235
ipv6 mld snooping enable....1236
ipv6 mld snooping explicit-tracking....1236
ipv6 mld snooping mrouter....1237
ipv6 mld snooping querier....1237
show ipv6 mld snooping groups....1238
show ipv6 mld snooping interface....1238
show ipv6 mld snooping mrouter....1239

35 Multicast Source Discovery Protocol (MSDP)....1241
clear ip msdp peer....1241
clear ip msdp sa-cache....1242
clear ip msdp statistic....1243
debug ip msdp....1244
ip msdp cache-rejected-sa....1244
ip msdp default-peer....1245
ip msdp log-adjacency-changes....1246
ip msdp mesh-group....1247

ip msdp originator-id....1247
ip msdp peer....1248
ip msdp redistribute....1250
ip msdp sa-filter....1250
ip msdp sa-limit....1251
ip msdp shutdown....1252
ip multicast-msdp....1253
show ip msdp....1253
show ip msdp sa-cache rejected-sa....1254

36 Multiple Spanning Tree Protocol (MSTP)....1256
debug spanning-tree mstp....1256
disable....1257
forward-delay....1258
hello-time....1259
max-age....1260
max-hops....1261
msti....1261
name....1262
protocol spanning-tree mstp....1263
revision....1264
show config....1265
show spanning-tree mst configuration....1266
show spanning-tree msti....1266
spanning-tree....1269
spanning-tree msti....1270
spanning-tree mstp edge-port....1271
tc-flush-standard....1272

37 Neighbor Discovery Protocol (NDP)....1273
debug ipv6 nd ra–guard....1274
device–role....1274
hop–limit....1275
ipv6 nd ra–guard attach–policy....1276
ipv6 nd ra–guard enable....1276
ipv6 nd ra–guard policy....1277
managed-config-flag....1277
match ra....1278
mtu....1279
other–config–flag....1279
reachable–time....1280
retrans-time....1281
router–lifetime....1281
router–preference maximum....1282
show config....1283
show ipv6 nd ra–guard policy....1284

trusted–port ... 1285

38 Object Tracking ... 1286
IPv4 Object Tracking Commands ... 1286
debug track ... 1286
delay ... 1287
description ... 1288
show running-config track ... 1289
show track ... 1290
threshold metric ... 1292
track interface ip routing ... 1293
track interface line-protocol ... 1294
track ip route metric threshold ... 1295
track ip route reachability ... 1296
track reachability refresh ... 1297
track resolution ip route ... 1298
IPv6 Object Tracking Commands ... 1299
show track ipv6 route ... 1300
track interface ipv6 routing ... 1301
track ipv6 route metric threshold ... 1302
track ipv6 route reachability ... 1304
track reachability refresh ... 1305
track resolution ipv6 route ... 1306

39 Open Shortest Path First (OSPFv2 and OSPFv3) ... 1308
OSPFv2 Commands ... 1308
area default-cost ... 1308
area nssa ... 1309
area range ... 1310
area stub ... 1311
auto-cost ... 1312
clear ip ospf ... 1313
clear ip ospf statistics ... 1313
debug ip ospf ... 1315
default-information originate ... 1317
default-metric ... 1318
description ... 1319
distance ... 1319
distance ospf ... 1320
distribute-list in ... 1321
distribute-list out ... 1322
enable inverse-mask ... 1323
fast-convergence ... 1324
graceful-restart grace-period ... 1325
graceful-restart helper-reject ... 1326
graceful-restart mode ... 1326

graceful-restart role....1327
ip ospf auth-change-wait-time....1328
ip ospf authentication-key....1329
ip ospf cost....1330
ip ospf dead-interval....1331
ip ospf hello-interval....1331
ip ospf message-digest-key....1332
ip ospf mtu-ignore....1333
ip ospf network....1334
ip ospf priority....1335
ip ospf retransmit-interval....1336
ip ospf transmit-delay....1337
log-adjacency-changes....1337
maximum-paths....1338
network area....1339
passive-interface....1340
redistribute....1342
redistribute bgp....1343
redistribute isis....1344
router-id....1345
router ospf....1346
show config....1347
show ip ospf....1348
show ip ospf asbr....1349
show ip ospf database....1350
show ip ospf database asbr-summary....1352
show ip ospf database external....1354
show ip ospf database network....1356
show ip ospf database nssa-external....1358
show ip ospf database opaque-area....1359
show ip ospf database opaque-as....1361
show ip ospf database opaque-link....1362
show ip ospf database router....1363
show ip ospf database summary....1366
show ip ospf interface....1368
show ip ospf neighbor....1370
show ip ospf routes....1371
show ip ospf statistics....1372
show ip ospf timers rate-limit....1376
show ip ospf topology....1377
summary-address....1378
timers spf....1379
timers throttle lsa all....1380
timers throttle lsa arrival....1381
OSPFv3 Commands....1381

area authentication....1382
area encryption....1383
area nssa....1385
auto-cost....1386
clear ipv6 ospf process....1386
clear ipv6 route....1387
debug ipv6 ospf bfd....1388
debug ipv6 ospf events....1389
debug ipv6 ospf packet....1391
debug ipv6 ospf spf....1392
default-information originate....1393
graceful-restart grace-period....1394
graceful-restart mode....1395
ipv6 neighbor....1396
ipv6 ospf area....1397
ipv6 ospf authentication....1398
ipv6 ospf bfd all-neighbors....1399
ipv6 ospf cost....1400
ipv6 ospf dead-interval....1401
ipv6 ospf encryption....1402
ipv6 ospf graceful-restart helper-reject....1404
ipv6 ospf hello-interval....1404
ipv6 ospf priority....1405
ipv6 router ospf....1406
maximum-paths....1407
passive-interface....1407
redistribute....1409
router-id....1410
show crypto ipsec policy....1411
show crypto ipsec sa ipv6....1413
show ipv6 ospf interface....1415
show ipv6 ospf database....1417
show ipv6 ospf neighbor....1419
snmp context....1420

40 PE Console Commands....1422
diag....1423
offline....1425
online....1426
power-cycle....1426
show control-bridge status....1427
show system....1428
telnet-peer-stack-unit....1432
upgrade system....1433

41 PE Stacking....1435

renumber....1435
reset....1436
show pe system....1438
show hardware pe....1441
stack unit....1443
stack-unit....1445

42 Per-VLAN Spanning Tree Plus (PVST+)....1446
description....1446
disable....1447
extend system-id....1448
protocol spanning-tree pvst....1449
show spanning-tree pvst....1450
spanning-tree pvst....1453
spanning-tree pvst err-disable....1455
tc-flush-standard....1456
vlan bridge-priority....1457
vlan forward-delay....1458
vlan hello-time....1459
vlan max-age....1460

43 PIM-Source Specific Mode (PIM-SSM)....1461
IPv4 PIM Commands....1461
clear ip pim tib....1461
debug ip pim....1462
ip pim dr-priority....1463
ip pim neighbor-filter....1464
ip pim query-interval....1465
show ip pim interface....1466
show ip pim neighbor....1467
show ip pim tib....1468
IPv4 PIM-Source Specific Mode Commands....1470
ip pim ssm-range....1470
show ip pim ssm-range....1471

44 PIM-Sparse Mode (PIM-SM)....1473
IPv4 PIM-Sparse Mode Commands....1473
clear ip pim rp-mapping....1473
clear ip pim tib....1474
debug ip pim....1475
ip pim bsr-border....1476
ip pim bsr-candidate....1477
ip pim dr-priority....1478
ip pim graceful-restart....1479
ip pim join-filter....1479
ip pim ingress-interface-map....1481

ip pim neighbor-filter....1481
ip pim query-interval....1482
ip pim register-filter....1483
ip pim rp-address....1484
ip pim rp-candidate....1485
ip pim sparse-mode....1486
ip pim spt-threshold....1487
ip pim sparse-mode sg-expiry-timer....1488
show ip pim bsr-router....1489
show ip pim snooping neighbor....1490
show ip pim interface....1491
show ip pim neighbor....1492
show ip pim rp....1493
show ip pim snooping interface....1494
show ip pim summary....1495
show ip pim tib....1497
show running-config pim....1499
IPv6 PIM-Sparse Mode Commands....1499
clear ipv6 pim tib....1499
debug ipv6 pim....1500
ipv6 pim bsr-border....1501
ipv6 pim bsr-candidate....1501
ipv6 pim dr-priority....1502
ipv6 pim query-interval....1502
ipv6 pim rp-address....1503
ipv6 pim rp-candidate....1504
ipv6 pim sparse-mode....1505
ipv6 pim sparse-mode sg-expiry-timer....1505
ipv6 pim spt-threshold....1506
show ipv6 pim bsr-router....1507
show ipv6 pim interface....1507
show ipv6 pim neighbor....1508
show ipv6 pim rp....1509
show ipv6 pim summary....1510
show ipv6 pim tib....1511

45 Policy-based Routing (PBR)....1513
ip redirect-group....1513
ip redirect-list....1514
permit....1515
redirect....1516
seq....1518
show cam pbr....1520
show ip redirect-list....1521

46 Port Extenders (PE)....1522

cascade interface....1523
clear pe statistics....1524
connect pe....1524
feature extended-bridge....1525
location-led....1526
pe....1527
pe provision....1528
pe-version-compat-support....1529
reset pe schedule....1530
reset pe range....1530
reset pe schedule show....1531
reset pe unschedule....1532
show config....1532
show ecid....1533
show pe....1535
show pe csp....1538
show pe errors....1539
Dual Homing....1540
batch-write-memory....1540
commit....1540
commit write....1541
discard....1542
import peer-config....1543
show config-mismatch....1544
show running-config local....1544
show running-config common....1545
show config....1546
write memory local....1547
Debugging....1547
clear hardware system-flow pe....1548
show software pemgr....1549
Power over Ethernet (PoE)....1559
advertise dot3-tlv....1559
advertise med power-via-mdi....1560
on-disable....1561
power budget global-threshold....1562
power inline....1563
power inline legacy....1564
power inline mode....1565
power inline restore pe....1566
power inline suspend pe....1567
upgrade poe-controller....1567
show power inline....1568
show power detail....1570
show revision....1570

47 Port Monitoring....1572
description....1572
erpm....1573
monitor session....1574
show config....1575
show monitor session....1576
show running-config monitor session....1577
source (port monitoring)....1578

48 Private VLAN (PVLAN)....1581
ip local-proxy-arp....1582
private-vlan mode....1583
private-vlan mapping secondary-vlan....1584
show interfaces private-vlan....1585
show vlan private-vlan....1586
switchport mode private-vlan....1589

49 Quality of Service (QoS)....1591
Global Configuration Commands....1591
qos-rate-adjust....1591
service-class bandwidth-percentage....1592
service-class dot1p-mapping....1593
service-class dynamic dot1p....1594
service-class wred backplane....1595
service-pool wred....1596
service-class wred ecn backplane....1598
show qos dot1p-queue-mapping....1599
Per-Port QoS Commands....1599
dot1p-priority....1599
rate police....1600
rate shape....1602
Policy-Based QoS Commands....1602
bandwidth-percentage....1603
buffer-stats-snapshot....1603
class-map....1604
clear qos statistics....1606
description....1607
match ip access-group....1608
match ip dscp....1609
match ip precedence....1610
match ip vlan....1611
match mac access-group....1612
match mac dot1p....1613
match mac vlan....1614
policy-aggregate....1614

policy-map-input....1615
policy-map-output....1616
qos-policy-input....1617
qos-policy-output....1619
rate-police....1620
rate-shape....1621
service-class buffer shared-threshold-weight....1622
service-policy input....1623
service-policy output....1624
service-queue....1625
set....1626
show qos class-map....1627
show qos policy-map....1628
show qos policy-map-input....1630
show qos policy-map-output....1631
show qos qos-policy-input....1632
show qos qos-policy-output....1633
show qos statistics....1634
show qos wred-profile....1635
threshold....1636
trust....1637
wred....1638
wred weight....1639
wred ecn....1640
wred-profile....1641
show hardware....1642
DSCP Color Map Commands....1643
dscp....1643
qos dscp-color-map....1644
qos dscp-color-policy....1645
show qos dscp-color-map....1646

50 Rapid Spanning Tree Protocol (RSTP)....1647
bridge-priority....1647
debug spanning-tree rstp....1648
description....1649
disable....1650
forward-delay....1650
hello-time....1651
max-age....1652
protocol spanning-tree rstp....1653
show config....1654
show spanning-tree rstp....1655
spanning-tree rstp....1657
tc-flush-standard....1659

51 Remote Monitoring (RMON)..... 1660
rmon alarm..... 1661
rmon collection history..... 1662
rmon collection statistics..... 1663
rmon event..... 1664
rmon hc-alarm..... 1665
show rmon..... 1666
show rmon alarms..... 1667
show rmon events..... 1668
show rmon hc-alarm..... 1669
show rmon history..... 1670
show rmon log..... 1671
show rmon statistics..... 1672

52 Routing Information Protocol (RIP)..... 1674
auto-summary..... 1675
clear ip rip..... 1675
debug ip rip..... 1676
default-information originate..... 1677
default-metric..... 1678
description..... 1679
distance..... 1679
distribute-list in..... 1680
distribute-list out..... 1681
ip poison-reverse..... 1682
ip rip receive version..... 1683
ip rip send version..... 1684
ip split-horizon..... 1685
maximum-paths..... 1685
neighbor..... 1686
network..... 1687
offset-list..... 1688
output-delay..... 1689
passive-interface..... 1690
redistribute..... 1691
redistribute isis..... 1692
redistribute ospf..... 1693
router rip..... 1694
show config..... 1695
show ip rip database..... 1695
show running-config rip..... 1697
timers basic..... 1697
version..... 1699

53 Security..... 1700

Role-Based Access Control Commands....1700
aaa authorization role-only 1701
role 1702
show role 1703
show userroles 1703
userrole 1704
AAA Accounting Commands....1705
aaa accounting....1705
aaa accounting suppress....1707
accounting....1708
show accounting....1709
Authorization and Privilege Commands....1709
authorization....1710
aaa authorization commands....1711
aaa authorization config-commands....1712
aaa authorization exec....1712
privilege level (CONFIGURATION mode)....1713
privilege level (LINE mode)....1714
Authentication and Password Commands....1715
aaa authentication enable....1715
aaa authentication login....1717
aaa reauthenticate enable....1718
access-class....1719
enable password....1720
enable sha256-password....1721
enable restricted....1722
enable secret....1723
login authentication....1724
password....1725
password-attributes....1726
service obscure-passwords....1727
service password-encryption....1728
secure-cli enable....1729
show privilege....1730
show users....1731
timeout login response....1732
username....1733
RADIUS Commands....1735
aaa radius auth-method....1735
client....1735
client-key....1736
coa-bounce-port....1737
coa-disable-port....1737
coa-reauthenticate....1738
debug radius....1738

da-rsp-timeout....1739
disconnect-user....1740
dynamic-auth-enable....1740
ip radius source-interface....1741
port....1742
radius dynamic-auth....1742
radius-server deadtime....1743
radius-server host....1744
radius-server key....1745
radius-server retransmit....1746
radius-server timeout....1747
rate-limit....1748
replay-protection-window....1748
terminate-session....1749
TACACS+ Commands....1749
debug tacacs+....1749
ip tacacs source-interface....1750
tacacs-server host....1751
tacacs-server key....1752
Port Authentication (802.1X) Commands....1753
dot1x authentication (Configuration)....1754
dot1x authentication (Interface)....1754
dot1x auth-fail-vlan....1755
dot1x auth-server....1756
dot1x guest-vlan....1757
dot1x mac-auth-bypass....1758
dot1x max-eap-req....1758
dot1x port-control....1759
dot1x quiet-period....1760
dot1x reauthentication....1761
dot1x reauth-max....1761
dot1x server-timeout....1762
dot1x supplicant-timeout....1763
dot1x tx-period....1764
show dot1x interface....1764
SSH Server and SCP Commands....1765
crypto cert generate....1766
crypto key generate....1767
crypto key zeroize rsa....1768
debug ip ssh....1768
ip scp topdir....1769
ip ssh authentication-retries....1770
ip ssh challenge–response–authentication....1771
ip ssh cipher....1771
ip ssh connection-rate-limit....1772

ip ssh hostbased-authentication....1773
ip ssh key-size....1774
ip ssh mac....1775
ip ssh password-authentication....1776
ip ssh pub-key-file....1777
ip ssh mac....1778
ip ssh rekey....1779
ip ssh rhostsfile....1779
ip ssh rsa-authentication (Config)....1780
ip ssh rsa-authentication (EXEC)....1781
ip ssh server....1782
ip ssh server dns enable....1785
ip ssh source-interface....1785
show crypto....1786
show ip ssh....1787
show ip ssh client-pub-keys....1788
show ip ssh rsa-authentication....1789
ssh....1790
Secure DHCP Commands....1792
clear ip dhcp snooping....1793
ip dhcp snooping....1793
ip dhcp snooping binding....1794
ip dhcp snooping database....1795
ip dhcp snooping database renew....1796
ip dhcp snooping trust....1796
ip dhcp source-address-validation....1797
ip dhcp snooping vlan....1797
show ip dhcp snooping....1798
ICMP Vulnerabilities....1799
drop icmp....1800
System Security Commands....1801
boot-access password....1801
generate hash....1802
root-access password....1802
verified boot hash....1803
verified startup-config....1804

54 Service Provider Bridging....1805
debug protocol-tunnel....1805
protocol-tunnel....1806
protocol-tunnel destination-mac....1807
protocol-tunnel enable....1808
protocol-tunnel rate-limit....1809
show protocol-tunnel....1810

55 sFlow....1811

sflow collector ... 1812
sflow enable (Global) ... 1814
sflow enable (Interface) ... 1815
sflow ingress-enable ... 1815
sflow extended-switch enable ... 1816
sflow max-header-size extended ... 1817
sflow polling-interval (Global) ... 1818
sflow polling-interval (Interface) ... 1819
sflow sample-rate (Global) ... 1820
sflow sample-rate (Interface) ... 1821
show sflow ... 1822
show sflow linecard ... 1823

56 Simple Network Management Protocol (SNMP) and Syslog ... 1825
SNMP Commands ... 1825
show snmp ... 1826
show snmp engineID ... 1827
show snmp group ... 1827
show snmp supported-mibs ... 1828
show snmp supported-traps ... 1829
show snmp user ... 1830
snmp context ... 1830
snmp ifmib ifalias long ... 1831
snmp mib community-map ... 1832
snmp-server contact ... 1832
snmp-server context ... 1833
snmp-server community ... 1834
snmp-server enable traps ... 1835
snmp-server engineID ... 1837
snmp-server group ... 1838
snmp-server host ... 1840
snmp-server location ... 1843
snmp-server packetsize ... 1844
snmp-server trap-source ... 1844
snmp-server user ... 1845
snmp-server view ... 1848
snmp-server vrf ... 1849
snmp trap link-status ... 1849
Syslog Commands ... 1850
clear logging ... 1850
clear logging auditlog ... 1851
default logging buffered ... 1851
default logging console ... 1852
default logging monitor ... 1853
default logging trap ... 1853
logging ... 1854

logging buffered 1855
logging console 1856
logging coredump stack-unit 1857
logging extended 1858
logging facility 1858
logging history 1860
logging history size 1861
logging monitor 1861
logging on 1862
logging source-interface 1863
logging synchronous 1864
logging trap 1865
logging version 1866
show logging 1867
show logging auditlog 1870
show logging driverlog 1871
show logging kernellog 1875
terminal monitor 1877

57 SNMP Traps 1878

58 Spanning Tree Protocol (STP) 1884
bpdu-destination-mac-address 1884
bridge-priority 1885
debug spanning-tree 1886
description 1887
disable 1887
forward-delay 1888
hello-time 1889
max-age 1890
protocol spanning-tree 1890
show config 1891
show spanning-tree 0 1892
spanning-tree 0 1895

59 Storm Control 1898
show storm-control broadcast 1899
show storm-control multicast 1900
show storm-control unknown-unicast 1901
storm-control broadcast (Configuration) 1902
storm-control broadcast (Interface) 1903
storm-control multicast (Configuration) 1903
storm-control multicast (Interface) 1904
storm-control pfc-llfc 1905
storm-control unknown-unicast (Configuration) 1905
storm-control unknown-unicast (Interface) 1906

60 SupportAssist 1908
eula-consent 1908
support-assist 1910
support-assist activate 1910
support-assist activity 1911
SupportAssist Commands 1911
activity 1912
contact-company 1912
contact-person 1913
enable 1914
server 1914
SupportAssist Activity Commands 1915
action-manifest get 1915
action-manifest install 1916
action-manifest remove 1917
action-manifest show 1917
enable 1918
SupportAssist Company Commands 1918
address 1919
street-address 1920
territory 1920
SupportAssist Person Commands 1921
email-address 1921
phone 1921
preferred-method 1922
time-zone 1923
SupportAssist Server Commands 1923
proxy-ip-address 1923
enable 1924
url 1925
show eula-consent 1925
show running-config 1927
show support-assist status 1927

61 System Time and Date 1929
clock set 1929
clock summer-time date 1930
clock summer-time recurring 1932
clock timezone 1933
debug ntp 1934
ntp authenticate 1935
ntp authentication-key 1935
ntp control-key-passwd 1937
ntp broadcast client 1937
ntp disable 1938

ntp master <stratum>..... 1939
ntp offset-threshold..... 1939
ntp server..... 1940
ntp source..... 1942
ntp trusted-key..... 1943
show clock..... 1944
show ntp associations..... 1945
show ntp status..... 1946
show ntp vrf associations..... 1948

62 Tunneling Commands..... 1949
ip unnumbered..... 1949
ipv6 unnumbered..... 1950
tunnel allow-remote..... 1951
tunnel destination..... 1952
tunnel dscp..... 1952
tunnel flow-label..... 1953
tunnel hop-limit..... 1954
tunnel keepalive..... 1954
tunnel-mode..... 1955
tunnel source..... 1956

63 Uplink Failure Detection (UFD)..... 1958
clear ufd-disable..... 1958
debug uplink-state-group..... 1959
description..... 1960
downstream..... 1960
downstream auto-recover..... 1962
downstream disable links..... 1962
enable..... 1963
show running-config uplink-state-group..... 1964
show uplink-state-group..... 1965
uplink-state-group..... 1966
upstream..... 1967

64 Virtual Link Trunking (VLT)..... 1969
back-up destination..... 1970
clear vlt statistics..... 1971
delay-restore..... 1972
lacp ungroup member-independent..... 1973
multicast peer-routing timeout..... 1974
peer-link port-channel..... 1974
peer-routing..... 1975
peer-routing-timeout..... 1976
primary-priority..... 1976
show vlt brief..... 1977

show vlt backup-link ... 1978
show vlt counters ... 1979
show vlt detail ... 1980
show vlt inconsistency ... 1981
show vlt mismatch ... 1982
show vlt private-vlan ... 1983
show vlt role ... 1984
show vlt statistics ... 1985
system-mac ... 1987
unit-id ... 1987
vlt domain ... 1988
vlt-peer-lag port-channel ... 1989
VLT Proxy Gateway ... 1990
peer-domain-link port-channel exclude-vlan ... 1990
proxy-gateway lldp ... 1991
proxy-gateway peer-timeout ... 1991
proxy-gateway static ... 1992
remote-mac-address exclude-vlan ... 1992
show vlt-proxy-gateway ... 1993
vlt-peer-mac transmit ... 1994

65 Virtual Router Redundancy Protocol (VRRP) ... 1996
IPv4 VRRP Commands ... 1996
advertise-interval ... 1996
authentication-type ... 1997
clear counters vrrp ... 1998
debug vrrp ... 1999
description ... 2000
disable ... 2001
hold-time ... 2001
preempt ... 2002
priority ... 2003
show config ... 2004
show vrrp ... 2005
version ... 2008
virtual-address ... 2009
vrrp delay minimum ... 2010
vrrp delay reload ... 2011
vrrp-group ... 2012
track ... 2013
IPv6 VRRP Commands ... 2014
clear counters vrrp ipv6 ... 2014
debug vrrp ipv6 ... 2015
show vrrp ipv6 ... 2016
vrrp-ipv6-group ... 2018

66 Virtual Routing and Forwarding (VRF)..... 2020
ip unknown-unicast..... 2020
ipv6 unknown-unicast..... 2020
description..... 2021
ip vrf forwarding..... 2022
ip route-export..... 2023
ip route-import..... 2024
ipv6 route-export..... 2024
ipv6 route-import..... 2025
match source-protocol..... 2026
redistribute..... 2027
interface management..... 2028
maximum dynamic-routes..... 2028
show ip vrf..... 2029
show run vrf..... 2030

67 VLAN Stacking..... 2032
member..... 2033
vlan-stack access..... 2034
vlan-stack compatible..... 2034
vlan-stack dot1p-mapping..... 2035
vlan-stack protocol-type..... 2036
vlan-stack trunk..... 2037

68 X.509v3..... 2040
crypto ca-cert delete..... 2040
crypto ca-cert install..... 2041
crypto cert delete..... 2042
crypto cert generate..... 2042
crypto cert install..... 2044
crypto x509 ocsp..... 2046
crypto x509 revocation..... 2046
debug crypto..... 2047
logging secure..... 2048
crypto x509 ca-keyid..... 2049
ocsp-server..... 2050
ocsp-server prefer..... 2050
show crypto ca-cert..... 2051
show crypto cert..... 2052

1

About this Guide

This CLI guide provides information about the Dell Networking operating system (OS) command-line interface (CLI) supported on a C9010 console to configure a C9010 switch, C1048P, N20xx, and N30xx port extenders. The C9010 switch is also referred to as network director or control bridge. The port extenders are also referred to as rapid access nodes.

This book also includes information about the protocols and features supported in the Dell Networking OS on the C9000 switch.

References

For more information about your system, go to the Dell Networking Support page and refer to the following documents:

- *Dell Networking C9000 Getting Started Guide*
- *Dell Networking C9000 Installation Guide*
- *Dell Networking C9000 Configuration Guide*
- *Dell Networking C9000 Release Notes*

Topics:

- Objectives
- Audience
- Conventions
- Information Icons

Objectives

This book is intended as a reference guide for CLI commands in the Dell Networking OS running on the C9000, with detailed syntax statements, usage information and sample output.

NOTE: For more information about when to use the CLI commands, see the *C9000 Configuration Guide* for your system.

Audience

This book is intended for system administrators who are responsible for configuring or maintaining networks. This guide assumes that you are knowledgeable in Layer 2 and Layer 3 networking technologies.

Conventions

This book uses the following conventions to describe command syntax.

`Keyword`	Keywords are in Courier and must be entered in the CLI as listed.
parameter	Parameters are in italics and require a number or word to be entered in the CLI.
{X}	Keywords and parameters within braces must be entered in the CLI.
[X]	Keywords and parameters within brackets are optional.

x|y	Keywords and parameters separated by a bar require you to choose one option.
x||y	Keywords and parameters separated by a double bar allows you to choose any or all of the options.

Information Icons

This book uses the following information symbols:

NOTE: The Note icon signals important operational information.

CAUTION: The Caution icon signals information about situations that could result in equipment damage or loss of data.

WARNING: The Warning icon signals information about hardware handling that could result in injury.

2

CLI Basics

This chapter describes the command line interface (CLI) structure and command modes. The Dell Networking operating software commands are in a text-based interface that allows you to use the launch commands, change command modes, and configure interfaces and protocols.

Topics:

- Accessing the Command Line
- Multiple Configuration Users
- Obtaining Help
- Navigating the CLI
- Using the Keyword no Command
- Filtering show Commands
- Command Modes

Accessing the Command Line

Once the system boots successfully, you are automatically placed in EXEC mode, and are not prompted to log in. You can access the commands through a serial console port or a Telnet session. When you Telnet into a switch, you are prompted to enter a login name and password.

Example

```
telnet 172.31.1.53
Trying 172.31.1.53...
Connected to 172.31.1.53.
Escape character is '^]'.
Login: username
Password: Dell>
```

After you log in to the switch, the prompt provides you with the current command-level information. For example:

Prompt	CLI Command Mode
Dell>	EXEC
Dell#	EXEC Privilege
Dell(conf)#	CONFIGURATION

NOTE: For a list of all the command mode prompts, see the Command Modes.

Multiple Configuration Users

When a user enters CONFIGURATION mode and another user is already in CONFIGURATION mode, the Dell Networking OS generates an alert warning message similar to the following:

```
Dell# conf

% Warning: The following users are currently configuring the system:

User "" on line console0
User "admin" on line vty0 ( 123.12.1.123 )
```

```
User "admin" on line vty1 ( 123.12.1.123 )
User "Irene" on line vty3 ( 123.12.1.321 )
Dell#conf
```

When another user enters CONFIGURATION mode, Dell Networking OS sends a message similar to the following:

```
% Warning: User "admin" on line vty2 "172.16.1.210" is in configuration
```

In this case, the user is “admin” on vty2.

Obtaining Help

As soon as you are in a command mode there are several ways to access help.

To obtain a list of keywords at any command mode:	Type a `?` at the prompt or after a keyword. There must always be a space before the `?`.
To obtain a list of keywords with a brief functional description:	Type `help` at the prompt.
To obtain a list of available options:	Type a keyword and then type a space and a `?`.
To obtain a list of partial keywords using a partial keyword:	Type a partial keyword and then type a `?`.
Example	The following is an example of typing `ip ?` at the prompt:

```
Dell(conf)# ?
aaa                             Authentication, Authorization and Accounting
arp                             Set a static ARP entry
asf-mode                        Enable Cut-Thru Mode
banner                          Define a login banner
bfd                             Configure BFD protocol
boot                            Modify system boot parameters
bpdu-destination-mac-address    Use Provider Bridge Address for xStp/Gvrp
cam-acl                         Configure CAM ACL
cam-audit                       Configure CAM auditing parameters
cam-acl-egress                  Configure Egress CAM ACL
cam-optimization                Optimize Cam utilization
class-map                       Configure Class Map for QoS
clock                           Configure time-of-day clock
configuration                   Enables exclusive configuration mode
crypto                          SSH key generation and IPSec policy
configuration
control-plane-cpuqos            Control plane CPU Qos configuration
default                         Set a command to its default
default-vlan                    Change flooding on default vlan
define                          Interface range macro definition
dot1x                           Configure 802.1x
ecmp-group                      ECMP group configuration
enable                          Modify enable password parameters
end                             Exit from configuration mode
ethernet                        Ethernet options
exit                            Exit from configuration mode
fastpatch                       Process runtime patch
fefd-global                     Enable FEFD globally
ftp-server                      FTP configuration subcommands
garp                            Configure GARP parameters
hash-algorithm                  Hash algorithm command
hg-link-bundle-monitor          Configure HiGig Link Bundle Monitoring
```

```
hostname                          Set system's network name
http-server                       Configure the HTTP server
interface                         Select an interface to configure
ip                                Global IP configuration subcommands
ipv6                              Global IPv6 configuration subcommands
lacp                              Configure LACP
line                              Configure a terminal line
linecard                          Configure linecard
link-bundle-distribution          Configure link-bundle
load-balance                      Global traffic load-balance configuration
logging                           Modify message logging facilities
mac                               Global MAC configuration subcommands
mac-address-table                 Mac Address Table Configuration Subcommands
management                        Create a management crypto or route, etc
monitor                           Monitor monitored ports
no                                Reset a command
ntp                               Configure NTP
openflow                          Configure OpenFlow instance
password-attributes               Configure password attributes
policy-map-input                  Configure input QoS policy map
policy-map-output                 Configure output QoS policy map
port-channel                      Configure port-channel group parameters
privilege                         Command privilege parameters
protocol                          Select a protocol to configure
protocol-tunnel                   Configure protocol tunneling
qos-policy-input                  Configure input QoS policy
qos-policy-output                 Configure output QoS policy
qos-rate-adjust                   Configure the number of bytes added to each
frame for rate policing/shaping
radius-server                     Set up RADIUS server
redundancy                        Set up linecard redundancy configuration
reload-type                       Configure the reload type
rmon                              Configure RMON alarm/event tables
route-map                         Create route-map or enter route-map command
mode
router                            Enable a routing process
script                            Start or stop a script
service                           Service selected component
service-class                     Define service class to policy based QoS/
Routing mapping
sflow                             sFlow configuration
snmp                              Modify SNMP parameters
snmp-server                       Modify SNMP parameters
storm-control                     Configure storm-control
strict-priority                   Configure a Queue as a strict priority queue
switch                            Configure Script CPU and Memory Limits
mount                             Mount target directory
tacacs-server                     Set up TACACS+ server
uplink-state-group                Uplink state group creation and configurations
username                          Establish user name authentication
util-threshold                    Cpu or memory utilization configurations
virtual-ip                        Virtual IP address
vlan-stack                        Vlan-stack command
vlt                               Enable Virtual Link Trunk
wred-profile                      Create a WRED profile
```

When entering commands, you can take advantage of the following timesaving features:The shortcut key combinations at the command line are as follows:

- The commands are not case-sensitive.
- You can enter partial (truncated) command keywords. For example, you can enter `int ten 0/1` for the `interface tengigabitethernet 0/1` command.
- To complete keywords in commands, use the TAB key.
- To display the last enabled command, use the up Arrow key.
- Use either the Backspace key or Delete key to erase the previous character.

- To navigate left or right in the command line, use the left and right Arrow keys.

Key Combination	Action
CNTL-A	Moves the cursor to the beginning of the command line.
CNTL-B	Moves the cursor back one character.
CNTL-D	Deletes the character at the cursor.
CNTL-E	Moves the cursor to the end of the line.
CNTL-F	Moves the cursor forward one character.
CNTL-I	Completes a keyword.
CNTL-K	Deletes all the characters from the cursor to the end of the command line.
CNTL-L	Re-enters the previous command.
CNTL-N	Returns to the more recent commands in the history buffer after recalling commands with Ctrl-P or the up Arrow key.
CNTL-P	Recalls commands, beginning with the last command.
CNTL-R	Re-enters the previous command.
CNTL-U	Deletes the line.
CNTL-W	Deletes the previous word.
CNTL-X	Deletes the line.
CNTL-Z	Ends continuous scrolling of the command outputs.
Esc B	Moves the cursor back one word.
Esc F	Moves the cursor forward one word.
Esc D	Deletes all the characters from the cursor to the end of the word.

Navigating the CLI

The Dell Networking operating software displays a CLI prompt comprised of the host name and CLI mode.

- Host name is the initial part of the prompt and is "Dell" by default. You can change the host name with the `hostname` command.
- CLI mode is the second part of the prompt and reflects the current CLI mode. For a list of the Dell Networking OS command modes, refer to the command mode list in the Accessing the Command Line section.

The CLI prompt changes as you move up and down the levels of the command structure. Starting with CONFIGURATION mode, the command prompt adds modifiers to further identify the mode. For more information about command modes, see the Command Modes section.

Using the Keyword no Command

To disable, delete or return to default values, use the `no` form of the commands.

For most commands, if you type the keyword `no` in front of the command, you disable that command or delete it from the running configuration. The `no` form of the command is described in the Syntax portion of the command description.

Filtering show Commands

To find specific information, display certain information only or begin the command output at the first instance of a regular expression or phrase, you can filter the display output of a `show` command.

When you execute a `show` command, and then enter a pipe (|), one of the following parameters, and a regular expression, the resulting output either excludes or includes those parameters.

NOTE: Dell Networking OS accepts a space before or after the pipe, no space before or after the pipe, or any combination. For example: `Dell#command | grep gigabit |except regular-expression | find regular-expression`

display	displays additional configuration information
except	displays only the text that does not match the pattern (or regular expression)
find	searches for the first occurrence of a pattern
grep	displays text that matches a pattern. The `grep` command option has an ignore-case suboption that makes the search case-insensitive. For example, the commands:

show run | grep Ethernet	returns a search result with instances containing a capitalized "Ethernet," such as `interface fortyGigE 0/0`
show run | grep ethernet	does not return the previous search result because it only searches for instances containing a noncapitalized "ethernet"
show run | grep Ethernet ignore-case	returns instances containing both "Ethernet" and "ethernet"

no-more	does not paginate the display output
save	copies the output to a file for future use

Displaying All Output

To display the output all at once (not one screen at a time), use the `no-more` option after the pipe. This operation is similar to the `terminal length screen-length` command except that the `no-more` option affects the output of just the specified command. For example: `Dell#show running-config|no-more`.

Filtering the Command Output Multiple Times

You can filter a single command output multiple times. To filter a command output multiple times, place the `save` option as the last filter. For example: `Dell# command | grep regular-expression | except regular-expression | grep other-regular-expression | find regular-expression | no-more | save`.

Command Modes

To navigate and launch various CLI modes, use specific commands. Navigation to these modes is described in the following sections.

BGP ADDRESS-FAMILY Mode

To enable or configure IPv4 or IPv6 for BGP, use BGP ADDRESS-FAMILY mode. For more information, see Border Gateway Protocol IPv4 (BGPv4).

To enter BGP ADDRESS-FAMILY mode:

1 Verify that you are logged in to ROUTER BGP mode.

2 Enter the command `address-family` then the protocol type (`ipv4 multicast` or `ipv6 unicast`). The prompt changes to include (conf-router_bgp_af) for IPv4 or (conf-router_bgpv6_af) for IPv6.

CLASS-MAP Mode

To create or configure a class map, use CLASS-MAP mode. For more information, see Policy-Based QoS Commands.

To enter CLASS-MAP mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `class-map` command then enter the class map name. The prompt changes to include (config-class-map).

You can return to CONFIGURATION mode by using the `exit` command.

CONFIGURATION Mode

In EXEC Privilege mode, use the `configure` command to enter CONFIGURATION mode and configure routing protocols and access interfaces.

To enter CONFIGURATION mode:

1 Verify that you are logged in to EXEC Privilege mode.

2 Enter the `configure` command. The prompt changes to include (conf).

From this mode, you can enter INTERFACE mode by using the `interface` command.

Configuration Terminal Batch Mode

To set up common configurations on a port extender connected in a dual homing environment, use Configuration Terminal Batch mode.

To enter Configuration Terminal Batch mode:

1 Verify that you are logged in to EXEC Privilege mode.

2 Enter the `configure terminal batch` command. The prompt changes to include (conf-b).

You can return to EXEC mode by using the `exit` command.

CONTROL-PLANE Mode

To manage control-plane traffic, use CONTROL-PLANE mode. For more information, see Control Plane Policing (CoPP).

To enter CONTROL-PLANE mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `control-plane-cpuqos` command. The prompt changes to include (conf-control-cpuqos).

You can return to CONFIGURATION mode by using the `exit` command.

DHCP Mode

To enable and configure Dynamic Host Configuration Protocol (DHCP), use DHCP mode. For more information, see Dynamic Host Configuration Protocol (DHCP).

To enter DHCP mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `ip dhcp server` command. The prompt changes to include (config-dhcp).

You can return to CONFIGURATION mode by using the `exit` command.

DHCP POOL Mode

To create an address pool, use DHCP POOL mode. For more information, see Dynamic Host Configuration Protocol (DHCP).

To enter DHCP POOL mode:

1 Verify that you are logged in to DHCP mode.

2 Enter the `pool` command then the pool name. The prompt changes to include (config-dhcp-*pool-name*).

You can return to DHCP mode by using the `exit` command.

ECMP GROUP Mode

To enable or configure traffic distribution monitoring on an ECMP link bundle, use ECMP GROUP mode. For more information, see ecmp_overview.

To enter ECMP GROUP mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `ecmp-group` command then enter the ECMP group ID. The prompt changes to include (conf-ecmp-group-*ecmp-group-id*).

You can return to CONFIGURATION mode by using the `exit` command.

EIS Mode

To enable or configure Egress Interface Selection (EIS), use EIS mode. For more information, see EIS Commands.

To enter EIS mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `management egress-interface-selection` command. The prompt changes to include (conf-mgmt-eis).

You can return to CONFIGURATION mode by using the `exit` command.

EXEC Mode

When you initially log in to the switch, by default, you are logged in to EXEC mode. This mode allows you to view settings and enter EXEC Privilege mode, which is used to configure the device.

When you are in EXEC mode, the > prompt is displayed following the host name prompt, which is "Dell" by default. You can change the host name prompt using the `hostname` command.

NOTE: Each mode prompt is preceded by the host name.

EXEC Privilege Mode

The `enable` command accesses EXEC Privilege mode. If an administrator has configured an "Enable" password, you are prompted to enter it.

EXEC Privilege mode allows you to access all the commands accessible in EXEC mode, plus other commands, such as to clear address resolution protocol (ARP) entries and IP addresses. In addition, you can access CONFIGURATION mode to configure interfaces, routes and protocols on the switch. While you are logged in to EXEC Privilege mode, the # prompt is displayed.

EXTENDED COMMUNITY LIST Mode

To enable and configure a BGP extended community, use EXTENDED COMMUNITY LIST mode. For more information, see BGP Extended Communities (RFC 4360).

To enter EXTENDED COMMUNITY LIST mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `ip extcommunity-list` command then a community list name. The prompt changes to include (conf-ext-community-list).

You can return to CONFIGURATION mode by using the `exit` command.

FRRP Mode

To enable or configure Force10 Resilient Ring Protocol (FRRP), use FRRP mode. For more information, see Force10 Resilient Ring Protocol (FRRP).

To enter FRRP mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `protocol frrp` command then the ring ID. The prompt changes to include (conf-frrp-*ring-id*).

You can return to CONFIGURATION mode by using the `exit` command.

GRUB Mode

To enable GRUB mode, press ESC when the following message appears during a system boot: `Press ESC key to stop autoreboot...`. Select `Force10 Boot` using the arrow keys and then press the "C" key to enter the GRUB Command Line Interface. The command prompt changes to `grub>`.

INTERFACE Mode

Use INTERFACE mode to configure interfaces or IP services on those interfaces. An interface can be physical (for example, a 10-Gigabit Ethernet port) or virtual (for example, the Null interface).

To enter INTERFACE mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `interface` command and then enter an interface type and interface number that is available on the switch.

The prompt changes to include the designated interface and slot/port number. For example:

Prompt	Interface Type
Dell(conf-if)#	INTERFACE mode
Dell(conf-if-te-0/0)#	Ten-Gigabit Ethernet interface then slot/port information
Dell(conf-if-fo-0/0)#	Forty-Gigabit Ethernet interface then slot/port information
Dell(conf-if-lo-0)#	Loopback interface number
Dell(conf-if-nu-0)#	Null Interface then zero
Dell(conf-if-pegi-0/0/1)#	Port Extender Gigabit Ethernet interface then pe-id/stack-unit/ port-id information.
Dell(conf-if-po-0)#	Port-channel interface number
Dell(conf-if-vl-0)#	VLAN Interface then VLAN number (range 1–4094)
Dell(conf-if-ma-0/0)#	Management Ethernet interface then slot/port information
Dell(conf-if-tu-0)#	Tunnel interface then tunnel ID.
Dell(conf-if-range)#	Designated interface range (used for bulk configuration).

IP ACCESS LIST Mode

To enter IP ACCESS LIST mode and configure either standard or extended access control lists (ACLs), use the `ip access-list standard` or `ip access-list extended` command.

To enter IP ACCESS LIST mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Use the `ip access-list standard` or `ip access-list extended` command. Include a name for the ACL. The prompt changes to include (conf-std-nacl) or (conf-ext-nacl).

You can return to CONFIGURATION mode by using the `exit` command.

LLDP Mode

To enable and configure Link Layer Discovery Protocol (LLDP), use LLDP mode. For more information, see Link Layer Discovery Protocol (LLDP).

To enter LLDP mode:

1 To enable LLDP globally, verify that you are logged in to CONFIGURATION mode. To enable LLDP on an interface, verify that you are logged in to INTERFACE mode.

2 Enter the `protocol lldp` command. The prompt changes to include (conf-lldp) or (conf-if-*interface*-lldp).

LLDP MANAGEMENT INTERFACE Mode

To enable and configure Link Layer Discovery Protocol (LLDP) on management interfaces, use LLDP MANAGEMENT INTERFACE mode. For more information, see the Link Layer Discovery Protocol (LLDP) chapter in the *Dell Networking OS Configuration Guide for the C9000 Series*.

To enter LLDP MANAGEMENT INTERFACE mode:

1 Verify that you are logged in to LLDP mode.

2 Enter the `management-interface` command. The prompt changes to include (conf-lldp-mgmtIf).

LINE Mode

To configure the console or virtual terminal parameters, use LINE mode.

To enter LINE mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `line` command. Include the keywords `console` or `vty` and their line number available on the switch. The prompt changes to include (config-line-console) or (config-line-vty).

You can exit this mode by using the `exit` command.

MAC ACCESS LIST Mode

To enter MAC ACCESS LIST mode and configure either standard or extended access control lists (ACLs), use the `mac access-list standard` or `mac access-list extended` command.

To enter MAC ACCESS LIST mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Use the `mac access-list standard` or `mac access-list extended` command. Include a name for the ACL. The prompt changes to include (conf-std-macl) or (conf-ext-macl).

You can return to CONFIGURATION mode by using the `exit` command.

MONITOR SESSION Mode

To enable and configure a traffic monitoring session using port monitoring, use MONITOR SESSION mode. For more information, see Port Monitoring.

To enter MONITOR SESSION mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `monitor session` command then the session ID. The prompt changes to include (conf-mon-sess-*sessionID*).

MULTIPLE SPANNING TREE (MSTP) Mode

To enable and configure MSTP, use MULTIPLE SPANNING TREE mode. For more information, see Multiple Spanning Tree Protocol (MSTP).

To enter MULTIPLE SPANNING TREE mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `protocol spanning-tree mstp` command. The prompt changes to include (conf-mstp).

You can return to CONFIGURATION mode by using the `exit` command.

PE Configuration Mode

To configure certain the port extender features such as, the PoE feature, use the PE CONFIGURATION mode. For more information, see the Port Extenders (PE)

To enter PE CONFIGURATION mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the`pe` *`pe-id`* command. The prompt changes to include (conf-pe *pe-id*)

Per-VLAN SPANNING TREE (PVST+) Plus Mode

To enable and configure the Per-VLAN Spanning Tree (PVST+) protocol, use PVST+ mode. For more information, see Per-VLAN Spanning Tree Plus (PVST+).

NOTE: The protocol name is PVST+, but the plus sign is dropped at the CLI prompt.

To enter PVST+ mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `protocol spanning-tree pvst` command. The prompt changes to include (conf-pvst).

You can return to CONFIGURATION mode by using the `exit` command.

PORT-CHANNEL FAILOVER-GROUP Mode

To configure shared LAG state tracking, use PORT-CHANNEL FAILOVER-GROUP mode. For more information, see Port Channel Commands.

To enter PORT-CHANNEL FAILOVER-GROUP mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `port-channel failover-group` command. The prompt changes to include (conf-po-failover-grp).

You can return to CONFIGURATION mode by using the `exit` command.

PREFIX-LIST Mode

To configure a prefix list, use PREFIX-LIST mode.

To enter PREFIX-LIST mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `ip prefix-list` command. Include a name for the prefix list. The prompt changes to include (conf-nprefixl).

You can return to CONFIGURATION mode by using the `exit` command.

PRIORITY GROUP Mode

To create an ETS priority group, use PRIORITY GROUP mode.

To enter PRIORITY GROUP mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `priority-group` command then the group name. The prompt changes to include (conf-pg).

You can return to CONFIGURATION mode by using the `exit` command.

PROTOCOL GVRP Mode

To enable and configure GARP VLAN Registration Protocol (GVRP), use PROTOCOL GVRP mode. For more information, see GARP VLAN Registration (GVRP).

To enter PROTOCOL GVRP mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `protocol gvrp` command. The prompt changes to include (config-gvrp).

You can return to CONFIGURATION mode by using the `exit` command.

QOS POLICY Mode

To configure ETS bandwidth allocation and scheduling for priority traffic, use QOS POLICY mode.

To enter QOS POLICY mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `qos-policy-output` command, then the policy name, then `ets`. The prompt changes to include (conf-qos-policy-out-ets).

You can return to CONFIGURATION mode by using the `exit` command.

RAPID SPANNING TREE (RSTP) Mode

To enable and configure RSTP, use RSTP mode. For more information, see Rapid Spanning Tree Protocol (RSTP).

To enter RSTP mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `protocol spanning-tree rstp` command. The prompt changes to include (conf-rstp).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTE-MAP Mode

To configure a route map, use ROUTE-MAP mode.

To enter ROUTE-MAP mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Use the `route-map` *`map-name`* `[permit | deny]` [*`sequence-number`*] command. The prompt changes to include (config-route-map).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTER BGP Mode

To enable and configure Border Gateway Protocol (BGP), use ROUTER BGP mode. For more information, see Border Gateway Protocol IPv4 (BGPv4)

To enter ROUTER BGP mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Use the `router bgp` command then enter the AS number. The prompt changes to include (conf-router_bgp).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTER OSPF Mode

To configure OSPF, use ROUTER OSPF mode. For more information, see Open Shortest Path First (OSPFv2).

To enter ROUTER OSPF mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `router ospf` {*`process-id`*} command. The prompt changes to include (conf-router_*ospf-id*).

You can switch to INTERFACE mode by using the `interface` command or you can switch to ROUTER RIP mode by using the `router rip` command.

ROUTER OSPFV3 Mode

To configure OSPF for IPv6, use ROUTER OSPFV3 mode. For more information, see Open Shortest Path First (OSPFv2 and OSPFv3).

To enter ROUTER OSPFV3 mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `ipv6 router ospf {process-id}` command. The prompt changes to include (conf-ipv6-router_ospf).

You can return to CONFIGURATION mode by using the `exit` command.

ROUTER RIP Mode

To enable and configure Router Information Protocol (RIP), use ROUTER RIP mode. For more information, see Routing Information Protocol (RIP).

To enter ROUTER RIP mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `router rip` command. The prompt changes to include (conf-router_rip).

You can return to CONFIGURATION mode by using the `exit` command.

SPANNING TREE Mode

To enable and configure the Spanning Tree protocol, use SPANNING TREE mode. For more information, see Spanning Tree Protocol (STP).

To enter SPANNING TREE mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `protocol spanning-tree` *stp-id* command. The prompt changes to include (conf-stp).

You can return to CONFIGURATION mode by using the `exit` command.

TRACE-LIST Mode

To configure a Trace list, use TRACE-LIST mode.

To enter TRACE-LIST mode:

1 Verify that you are logged in to CONFIGURATION mode.
2 Enter the `ip trace-list` command. Include the name of the Trace list. The prompt changes to include (conf-trace-acl).

You can exit this mode by using the `exit` command.

VRRP Mode

To enable and configure Virtual Router Redundancy Protocol (VRRP), use VRRP mode. For more information, see Virtual Router Redundancy Protocol (VRRP).

To enter VRRP mode:

1 To enable VRRP globally, verify that you are logged in to CONFIGURATION mode.
2 Enter the `vrrp-group` command then enter the VRRP group ID. The prompt changes to include (conf-if-*interface-type-slot/port*-vrid-*vrrp-group-id*).

UPLINK STATE GROUP Mode

To enable and configure an uplink-state group, use UPLINK STATE GROUP mode. For more information, see Uplink Failure Detection (UFD).

To enter UPLINK STATE GROUP mode:

1 Verify that you are logged in to CONFIGURATION mode.

2 Enter the `uplink-state-group` command then the group ID number. The prompt changes to include (conf-uplink-state-group-*groupID*).

3

Control and Monitoring

This chapter contains the commands to configure and monitor the system, including Telnet, file transfer protocol (FTP), and trivial file transfer protocol (TFTP) as they are implemented in the Dell Networking OS on the switch.

Topics:

- asf-mode
- banner exec
- banner login
- banner motd
- cam-acl
- cam-audit linecard
- clear alarms
- clear average-power
- clear line
- configure
- debug cpu-traffic-stats
- debug ftpserver
- disable
- do
- enable
- enable cpu-clock-monitor
- enable optic-info-update interval
- end
- exec-timeout
- exit
- ftp-server enable
- ftp-server topdir
- ftp-server username
- hostname
- ip ftp password
- ip ftp source-interface
- ip ftp username
- ip http source-interface
- ip telnet server enable
- ip telnet source-interface
- ip tftp source-interface
- line
- logging coredump server
- login concurrent-session
- login statistics
- ping

- power on
- reload
- send
- service timestamps
- show alarms
- show asf
- show chassis
- show command-history
- show console lp
- show cpu-traffic-stats
- show cpu-interface-stats
- show debugging
- show environment
- show inventory
- show linecard
- show login statistics
- show memory
- show processes cpu
- show processes ipc
- show processes ipc flow-control
- show processes memory
- show reset-reason
- show rpm
- show software ifm
- show system linecard
- show tech-support
- show util-threshold cpu
- show util-threshold memory
- show version
- telnet
- terminal length
- traceroute
- undebug all
- upload trace-log
- util-threshold cpu
- util-threshold memory
- virtual-ip
- write

asf-mode

Enable the transmission of Alternate Store and Forward (ASF) packets as soon as a threshold is reached.

C9000 Series

Syntax `asf-mode linecard {`*`slot-id`* `| all}`

To return to standard Store and Forward mode, use the `no asf-mode linecard` command.

Parameters

linecard *slot-id*	Enter the slot ID of a switch line card. The range of slot IDs is from 0 to 11. Enter `all` to enable ASF mode on all line cards on the switch.

Defaults Not configured

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information You *must* save the configuration and reload the system to implement ASF. When you enter the command, the system sends a message stating that the new mode is enabled when the system reloads.

banner exec

Configure a message that is displayed when your enter EXEC mode.

C9000 Series

Syntax `banner exec c line c`

To delete a banner, use the `no banner exec` command.

Parameters

c	Enter the keywords `banner exec`, then enter a character delineator, represented here by the letter *c*. Press **ENTER**.
line	Enter a text string for your banner message ending the message with your delineator. In the following example, the delineator is a percent character (%); the banner message is "testing, testing".

Defaults No banner is displayed.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original Command

Usage Information After entering the `banner exec` command, type one or more spaces and a delineator character. Enter the banner text then the second delineator character. When you connect to the router, if a message of the day banner is configured, it displays first. If no message of the day banner is configured, the login banner and prompt appear. After logged in, the EXEC banner (if configured) displays.

Example

```
Dell(conf)#banner exec ?
LINE c banner-text c, where 'c' is a delimiting character
Dell(conf)#banner exec %
Enter TEXT message. End with the character '%'.
This is the banner%
Dell(conf)#end
Dell#exit
4d21h5m: %RPM0-P:CP %SEC-5-LOGOUT: Exec session is terminated for user on line
console

This is the banner

Dell Networking OS con0 now available

Press RETURN to get started.
4d21h6m: %RPM0-P:CP %SEC-5-LOGIN_SUCCESS: Login successful for user on line
console
This is the banner
Dell>
```

Related Commands line — enables and configures the console and virtual terminal lines to the system.

banner login

Set a banner to display when logging on to the system.

C9000 Series

Syntax `banner login {acknowledgement | keyboard-interactive | no keyboard-interactive} [c line c]`

Parameters

keyboard-interactive	Enter the keyword `keyboard-interactive` to require a carriage return (CR) to get the message banner prompt.

acknowledgement	Enter the `acknowledgement` keyword to require a positive acknowledgement from the user while logging in to the system.
c	Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).
line	Enter a text string for your text banner message ending the message with your delineator. The delineator is a percent character (%). Range: maximum of 50 lines, up to 255 characters per line

Defaults No banner is configured and the CR is required when creating a banner.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the `acknowledgement` keyword.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced the keyword `keyboard-interactive`.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

Usage Information After entering the banner login command, type one or more spaces and a delineator character. Enter the banner text then the second delineator character. When the user is connected to the router, if a message of the day banner is configured, it displays first. If no message of the day banner is configured, the login banner and prompt appear. After the user has logged in, the EXEC banner (if configured) displays.

Example

```
Dell(conf)#banner login ?
acknowledgement         Require positive acknowledgment after login prompt
keyboard-interactive     Press enter key to get prompt
LINE                 c banner-text(max length 255) c, where 'c' is a
delimiting character
Dell(conf)#no banner login ?
acknowledgement         Disable positive acknowledgment required after login
prompt
keyboard-interactive     Prompt will be displayed by default
```

If you configure the `acknowledgement` keyword, the system requires a positive acknowledgement from the user while logging in to the system.

```
$ telnet 10.11.178.16
Trying 10.11.178.16...
Connected to 10.11.178.16.
Escape character is '^]'.
```

```
THIS IS A LOGIN BANNER. PRESS 'Y' TO ACKNOWLEDGE. ACKNOWLEDGE?

[y/n]: y
Login: admin
Password:
```

Related Commands banner motd — sets a Message of the Day banner.

banner motd

Set a message of the day (MOTD) banner.

C9000 Series

Syntax `banner motd c line c`

Parameters

c	Enter a delineator character to specify the limits of the text banner. The delineator is a percent character (%).
line	Enter a text string for your MOTD banner the message with your delineator. The delineator is a percent character (%).

Defaults No banner is configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

Usage Information After entering the banner login command, type one or more spaces and a delineator character. Enter the banner text then the second delineator character. When the user is connected to the router, if a message of the day banner is configured, it displays first. If no message of the day banner is configured, the login banner and prompt appear. After the user has logged in, the EXEC banner (if configured) displays.

Related Commands

- banner exec — enables the display of a text string when you enter EXEC mode.

- banner login — sets a banner to display after successful login to the system.

cam-acl

Allocate content addressable memory (CAM) for IPv4 and IPv6 ACLs.

C9000 Series

Syntax

```
cam-acl {default | l2acl number{ ipv4acl number ipv6acl number ipv4qos number
l2qos number l2pt number ipmacacl number vman-qos | vman-dual-qos number
ecfmacl number [ openflow number fcoeacl number | fedgovacl number|
nlbclusteracl number | ipv4pbr number | iscsioptaclnumber | openflow number |
vrfv4ac numberl ]}}
```

Parameters

default Use the default CAM profile settings and set the CAM as follows:

- L3 ACL (ipv4acl): 4
- L2 ACL(l2acl): 5
- IPv6 L3 ACL (ipv6acl): 0
- L3 QoS (ipv4qos): 2
- L2 QoS (l2qos): 1
- OpenFlow: 0 (disabled)
- FCoE (fcoeacl): 0 (disabled)
- iSCSI Optimization (iscsioptacl): 0 (disabled)
- L2 PT : 0
- IP-MAC ACL : 0
- Vman QoS : 0
- ECFM ACL: 0
- IPv4 PBR : 0
- VRFv4 ACL : 0
- FedGov ACL : 0
- NLB Cluster ACL : 0

l2acl *number* Allocate space to each CAM region.

Enter the CAM profile name then the amount for CAM space allocation. The total space allocated must be equal to 12. The IPv6 ACL range must be a factor of 2.

Enter `l2acl` and the FP block *number* for L2 ACL. The FP block number range is from 1 to 8.

- `4`: Creates 242 entries for use by the OpenFlow controller (256 total entries minus the 14 entries reserved for internal functionality)
- `8`: Creates 498 entries for use by the OpenFlow controller (512 total entries minus the 14 entries reserved for internal functionality)

ipv4acl *number* Enter `ipv4acl` and the FP block *number* for IPv4. The FP block number range is from 0 to 8.

ipv6acl *number*	Enter `ipv6acl` and the FP block *number* for IPv6. The FP block number range is from 0 to 4 (multiples of 2).
ipv4qos *number*	Enter `ipv4qos` and the FP block *number* for IPv4–QoS. The FP block number range is from 0 to 8.
l2qos *number*	Enter `l2qos` and the FP block *number* for L2–QoS. The FP block number range is from 1 to 8.
l2pt *number*	Enter `l2pt` and the FP block *number* for L2–Protocol tunneling. The FP block number range is from 0 to 1.
ipmacacl *number*	Enter `ipmacacl` and the FP block *number* for IP-MAC ACL. The FP block number range is from 0 to 6.
vman-qos *number*	Enter `vman-qos` and the FP block *number* for Vman QoS. The FP block number range is from 0 to 6.
ecfmacl *number*	Enter `ecfmacl` and the FP block *number* for ECFM ACL. The FP block number range is from 0 to 5.
fcoeacl *number*	Enter `fcoeacl` and the FP block *number* for FCoE ACL. The FP block number range is 0 to 6.
fedgovacl *number*	Enter `fedgovacl` and the FP block *number* for Fed Gov ACL. The FP block number range is 0 to .
nlbclusteracl *number*	Enter `nlbclusteracl` and the FP block *number* for NLB Cluster ACL. The FP block number range is 0 to 6.
ipv4pbr *number*	Enter `ipv4pbr` and the FP block *number* for IPv4 PBR ACL. The FP block number range is 0 to 6.
iscsioptacl *number*	Enter `iscsioptacl` and the FP block *number* for ISCSI optimization ACL. The FP block number range is 0 to 6.
openflow *number*	Enter `openflow` and the FP block *number* for OpenFlow ACL. The FP block number range is 0 to 6.
vrfv4acl *number*	Enter `vrfv4acl` and the FP block *number* for VRF ACL. The FP block number range is 0 to 6.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Added support for the `fcoe` parameter on the S4810 and S4820T.
9.1.(0.0)	Added support for OpenFlow on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Added the keywords `fcoeacl` and `iscsioptacl` on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Added the keywords `ecfmacl`, `vman-qos`, and `vman-dual-qos`.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.

Usage Information

For the new settings to take effect, save the new CAM settings to the startup-config (`write-mem` or `copy run start`) then reload the system.

The total amount of space allowed is 16 FP Blocks. System flow requires four blocks and these blocks cannot be reallocated. The total number of blocks must be equal to 12. The `ipv4acl` profile range is from 0 to 8.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 12.

Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl` profile which is from 0 to 10. The `ipv6acl` allocation must be a factor of 2 (2, 4, 6, 8, 10).

If you enabled BMP 3.0, to perform a reload on the chassis to upgrade any configuration changes that have changed the NVRAM content, use the `reload conditional nvram-cfg-change` command.

You can use the `cam-acl default` command in Configuration Terminal Batch mode to reset ACL CAM entries to default settings in a dual-homing setup.

cam-audit linecard

Enable audit of the IPv4 forwarding table on all line cards.

C9000 Series

Syntax `cam-audit linecard all ipv4-fib interval` *`time-in-minutes`*

Parameters

all	Enter the keyword `all` to enable CAM audit on all line cards.

	ipv4-fib	Enter the keyword `ipv4-fib` to designate the CAM audit on the IPv4 forwarding entries.
	interval *time-in-minutes*	Enter the keyword `interval` followed by the frequency in minutes of the CAM audit. Range: 5 to 1440 minutes (24 hours). Default: **60 minutes**.

Defaults Disabled

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced on the E-Series.

Usage Information Enables periodic audits of the software and hardware copies of the IPv4 forwarding table. Use this command in Configuration Terminal Batch mode to enable the audits in the chassis connected in a dual-homing setup.

clear alarms

Clear alarms on the system.

C9000 Series

Syntax `clear alarms`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
E-Series	Original command.

Usage Information This command clears alarms that are no longer active. If an alarm situation is still active, it is seen in the system output.

clear average-power

Reset the average power and average power start time.

Syntax `clear average-power stack-unit {stack-unit-number}`

Parameters

stack-unit-number	Enter the stack unit number.

Defaults None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(2.1P1)	Introduced on all Dell EMC Networking OS platforms

Usage Information This command resets the average power and average power start time to the current time. Average power and average power start time will be calculated from the reset time (i.e current time).

Example This output is only applicable for the C1048P, N20xx and N30xx.

```
DellEMC#clear average-power pe 2 stack-unit  3
Proceed to clear Average power ? Confirm [yes/no]:yes
DellEMC#
```

This output is only applicable for the C9000 platform (not the port extenders).

```
DellEMC#clear average-power
Proceed to clear Average power ? Confirm [yes/no]:yes
DellEMC#
```

clear line

Reset a terminal line.

C9000 Series

Syntax `clear line {line-number | console 0 | vty number}`

Parameters

line-number	Enter a number for one of the 12 terminal lines on the system. The range is from 0 to 11.
console 0	Enter the keywords `console 0` to reset the console port.

	vty number	Enter the keyword `vty` then a number to clear a terminal line. The range is from 0 to 9.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

configure

Enter CONFIGURATION mode from EXEC Privilege mode.

C9000 Series

Syntax `configure [terminal]`

Parameters

terminal	(OPTIONAL) Enter the keyword `terminal` to specify that you are configuring from the terminal.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Example

```
Dell#configure
Dell(conf)#
```

debug cpu-traffic-stats

Enable the collection of computer processor unit (CPU) traffic statistics.

C9000 Series

Syntax

`debug cpu-traffic-stats`

To disable the debugging, use the `no debug cpu-traffic-stats` command.

Defaults

Disabled

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

This command enables (and disables) the collection of CPU traffic statistics from the time this command is executed (not from system boot). However, excessive traffic a CPU receives automatically triggers (turn on) the collection of CPU traffic statics.

The following message is an indication that collection of CPU traffic is automatically turned on. To view the traffic statistics, use the `show cpu-traffic-stats` command.

If the CPU receives excessive traffic, traffic is rate controlled.

NOTE: This command must be enabled before the `show cpu-traffic-stats` command displays traffic statistics. Dell Networking recommends disabling debugging (`no debug cpu-traffic-stats`) after troubleshooting is complete.

Related Commands show cpu-traffic-stats — displays the cpu traffic statistics.

debug ftpserver

View transactions during an FTP session when a user is logged into the FTP server.

C9000 Series

Syntax `debug ftpserver`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

disable

Return to EXEC mode.

C9000 Series

Syntax `disable [level]`

From a **port extender (PE) console**, use `disable [level]` to return to EXEC mode.

Parameters

level	(OPTIONAL) Enter a number for a privilege level of the Dell Networking OS. The range is from 0 to 15. The default is **1**.

Defaults **1**

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information You can also use the `disable` command from port extender(PE) console to turns off access to the privileged mode commands.

do

Allow the execution of most EXEC-level commands from all CONFIGURATION levels without returning to the EXEC level.

C9000 Series

Syntax `do command`

Parameters

command	Enter an EXEC-level command.

Defaults none

Command Modes

- CONFIGURATION
- INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The following commands are *not* supported by the `do` command:

- `enable`
- `disable`
- `exit`
- `config`

Example

```
Dell(conf-if-te-5/0)#do clear counters
Clear counters on all interfaces [confirm]
Dell(conf-if-te-5/0)#
Dell(conf-if-te-5/0)#do clear logging
Clear logging buffer [confirm]
Dell(conf-if-te-5/0)#
Dell(conf-if-te-5/0)#do reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload [confirm yes/no]: n
Dell(conf-if-te-5/0)#
```

enable

Enter EXEC Privilege mode or any other privilege level configured. After entering this command, you may need to enter a password.

C9000 Series

Syntax `enable [level]`

From a **PE console**, use `enable [level]` to enter EXEC privilege mode .

Parameters

level	(OPTIONAL) Enter a number for a privilege level of Dell Networking OS. The range is from 0 to 15.

Defaults **15**

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

Users entering EXEC Privilege mode or any other configured privilege level can access configuration commands. To protect against unauthorized access, use the `enable password` command to configure a password for the `enable` command at a specific privilege level. If no privilege level is specified, the default is privilege level **15**. You can also use the `enable [level]` command from a PE console to enter the privileged mode.

NOTE: If you are authorized for the EXEC Privilege mode by your role, you do not need to enter an enable password.

Related Commands

enable password — configures a password for the `enable` command and to access a privilege level.

enable cpu-clock-monitor

Enables Intel CPU LPC (Low Pin Count) clock-failure monitoring.

Syntax

`enable cpu-clock-monitor`

To disable this feature, use the `no enable cpu-clock-monitor` command.

Parameters

None

Defaults

Enabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(2.0P2)	Introduced on the C9010, S3048–ON, S6100–ON and Z9100–ON.

Usage Information Enables Intel CPU LPC (Low Pin Count) clock-failure monitoring and issues a warning syslog to the user to take appropriate action if signal degradation is seen.

enable optic-info-update interval

Enable polling intervals of optical information updates for simple network management protocol (SNMP).

C9000 Series

Syntax `enable optical-info-update interval` *seconds*

To disable optical power information updates, use the `no enable optical-info-update interval` command.

Parameters

interval *seconds* Enter the keyword `interval` then the polling interval in seconds. The range is from 120 to 6000 seconds. The default is **300 seconds** (5 minutes).

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Replacement command for the S4820T. Replaces the `enable xfp-power-updates` command.
8.3.11.4	Replacement command for the Z9000. Replaces the `enable xfp-power-updates` command
8.3.10.0	Replacement command for the S4810 only. Replaces the `enable xfp-power-updates` command.

Usage Information To enable polling and to configure the polling frequency, use this command.

end

Return to EXEC Privilege mode from other command modes (for example, CONFIGURATION or ROUTER OSPF modes).

C9000 Series

Syntax `end`

Command Modes

- CONFIGURATION
- SPANNING TREE
- MULTIPLE SPANNING TREE
- LINE
- INTERFACE
- TRACE-LIST
- VRRP
- ACCESS-LIST
- PREFIX-LIST
- AS-PATH ACL
- COMMUNITY-LIST
- ROUTER OSPF
- ROUTER RIP
- ROUTER ISIS
- ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.
E-Series	Original command.

Related Commands

exit — returns to the lower command mode.

exec-timeout

Set a time interval that the system waits for input on a line before disconnecting the session.

C9000 Series

Syntax

`exec-timeout` *minutes* [*seconds*]

To return to default settings, use the `no exec-timeout` command.

Parameters

minutes	Enter the number of minutes of inactivity on the system before disconnecting the current session. The range is from 0 to 35791. The default is **10 minutes** for the console line and **30 minutes** for the VTY line.
seconds	(OPTIONAL) Enter the number of seconds. The range is from 0 to 2147483. The default is **0 seconds**.

Defaults **10 minutes** for console line; **30 minutes** for VTY lines; **0 seconds**

Command Modes LINE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information To remove the time interval, enter `exec-timeout 0 0`.

Example

```
Dell Networking OS con0 is now available
Press RETURN to get started.
Dell>
```

exit

Return to the lower command mode.

C9000 Series

Syntax `exit`

From a **PE console**, use `exit` command to return to the lower command mode.

Command Modes

- EXEC Privilege
- CONFIGURATION
- LINE, INTERFACE
- TRACE-LIST
- PROTOCOL GVRP

- SPANNING TREE
- MULTIPLE SPANNING TREE
- MAC ACCESS LIST
- ACCESS-LIST
- AS-PATH ACL
- COMMUNITY-LIST
- PREFIX-LIST
- ROUTER OSPF
- ROUTER RIP
- ROUTER ISIS
- ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Related Commands end — returns to EXEC Privilege mode.

ftp-server enable

Enable FTP server functions on the system.

C9000 Series

Syntax `ftp-server enable`

Defaults Disabled

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Example

```
morpheus% ftp 10.31.1.111
Connected to 10.31.1.111.
220 FTOS (1.0) FTP server ready
Name (10.31.1.111:dch): dch
331 Password required
Password:
230 User logged in
ftp> pwd
257 Current directory is "flash:"
ftp> dir
200 Port set okay
150 Opening ASCII mode data connection
size  date       time name
-------- ------ ------ --------
 512  Jul-20-2004  18:15:00 tgtimg
 512  Jul-20-2004  18:15:00 diagnostic
 512  Jul-20-2004  18:15:00 other
 512  Jul-20-2004  18:15:00 tgt
226 Transfer complete
329 bytes received in 0.018 seconds (17.95 Kbytes/s)
ftp>
```

Related Commands

ftp-server topdir — sets the directory to be used for incoming FTP connections to the E-Series.

ftp-server username — sets a username and password for incoming FTP connections to the E-Series.

ftp-server topdir

Specify the top-level directory to be accessed when an incoming FTP connection request is made.

C9000 Series

Syntax `ftp-server topdir directory`

Parameters

directory	Enter the directory path.

Defaults The internal flash is the default directory.

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

After you enable FTP server functions with the `ftp-server enable` command, Dell Networking recommends specifying a top-level directory path. Without a top-level directory path specified, the system directs users to the flash directory when logging in to the FTP server.

Related Commands

ftp-server enable — enables FTP server functions on the switch.

ftp-server username — sets a username and password for incoming FTP connections.

ftp-server username

Create a user name and associated password for incoming FTP server sessions.

C9000 Series

Syntax

`ftp-server username` *`username`* `password [`*`encryption-type`*`]` *`password`*

To delete a user name and its password, use the `no ftp-server username username` command.

Parameters

username	Enter a text string up to 40 characters long as the user name.
password *password*	Enter the keyword `password` then a string up to 40 characters long as the password. Without specifying an encryption type, the password is unencrypted.
encryption-type	(OPTIONAL) After the keyword `password`, enter one of the following numbers: • `0` (zero) for an unecrypted (clear text) password • `7` (seven) for a hidden text password

Defaults

Not enabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

hostname

Manually set a desired host name for the system.

C9000 Series

Syntax `hostname` *`name`*

From a **PE console**, use `hostname` *`name`* to set a PE system host name.

To unconfigure a hostname configured for a PE, use `no hostname`

Parameters

name	Enter a text string, up to 32 characters long.

Defaults **Dell Networking OS**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.12.0	Changed the default from Force10 to FTOS.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

The host name is used in the command-line prompt.

To configure a desired PE console hostname, use the `hostname` command from a PE console.

To unconfigure the hostname configured for the PE console, use `no hostname`. If no hostnames are configured, the system. uses the default hostname, "Dell".

Example (PE Console)

```
Dell#hostname PE1
PE1#
```

ip ftp password

Specify a password for outgoing FTP connections.

C9000 Series

Syntax

`ip ftp password [encryption-type] password`

To remove a password and return to the default setting, use the `no ip ftp password [password]` command.

Parameters

encryption-type	(OPTIONAL) Enter one of the following numbers: • 0 (zero) for an unecrypted (clear text) password • 7 (seven) for a hidden text password
password	Enter a string up to 40 characters as the password.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information The password is listed in the configuration file; you can view the password by entering the `show running-config ftp` command.

Use the `ip ftp password` command when you use the `ftp: parameter` in the `copy` command.

Related Commands ip ftp username — sets the user name for the FTP sessions.

ip ftp source-interface

Configure an interface's IP address as the source IP address for FTP connections.

C9000 Series

Syntax `ip ftp source-interface` *interface*

To delete an interface, use the `no ip ftp source-interface` *interface* command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel`.

Defaults The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Increased number of VLANs on ExaScale to 4094 (was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

ip ftp username

Assign a user name for outgoing FTP connection requests.

C9000 Series

Syntax

`ip ftp username` *`username`*

To return to anonymous FTP connections, use the `no ip ftp username [`*`username`*`]` command.

Parameters

username	Enter a text string as the user name up to 40 characters long.

Defaults

No user name is configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information Configure a password with the `ip ftp password` command.

Related Commands ip ftp password — sets the password for FTP connections.

ip http source-interface

Configure an interface's IP address as the source IP address for HTTP connections.

C9000 Series

Syntax `ip http source-interface` *interface*

To delete an interface, use the`no ip http source-interface` *interface* command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel`.

Defaults The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.

Version	Description
9.3(0.1)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.3.11.1	Introduced on the Z9000
8.2.1.0	Increased number of VLANs on ExaScale to 4094 (was 2094)
8.1.1.0	Introduced on E-Series ExaScale
7.6.1.0	Support added for S-Series
7.5.1.0	Introduced on C-Series

ip telnet server enable

Enable the Telnet server on the switch.

C9000 Series

Syntax

```
ip telnet server enable
```

To disable the Telnet server, use the `no ip telnet server enable` command.

Defaults Enabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands ip ssh server — enables the secure shell (SSH) server on the system.

ip telnet source-interface

Set an interface's IP address as the source address in outgoing packets for Telnet sessions.

C9000 Series

Syntax

`ip telnet source-interface` *interface*

To return to the default setting, use the `no ip telnet source-interface [`*interface*`]` command.

Parameters

interface — Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel, enter the keyword `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel`.

Defaults

The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Increased number of VLANs on ExaScale to 4094 (was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

Related Commands telnet — telnets to another device.

ip tftp source-interface

Assign an interface's IP address in outgoing packets for TFTP traffic.

C9000 Series

Syntax

`ip tftp source-interface` *interface*

To return to the default setting, use the `no ip tftp source-interface` *interface* command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel, enter the keyword `port-channel` then a number. The range is 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults The IP address on the system that is closest to the Telnet address is used in the outgoing packets.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4820T.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Increased number of VLANs on ExaScale to 4094 (was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

line

Enable and configure console and virtual terminal lines to the system. This command accesses LINE mode, where you can set the access conditions for the designated line.

C9000 Series

Syntax `line {console 0 | vty number [end-number]}`

Parameters

console 0	Enter the keyword `console 0` to configure the console port. The console option for the S-Series is `<0-0>`.
vty *number*	Enter the keyword `vty` then a number from 0 to 9 to configure a virtual terminal line for Telnet sessions. The system supports 10 Telnet sessions.
end-number	(OPTIONAL) Enter a number from 1 to 9 as the last virtual terminal line to configure. You can configure multiple lines at one time.

Defaults Not configured

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

Usage Information You cannot delete a terminal connection.

Related Commands access-class — restricts the incoming connections to a particular IP address in an IP access control list (ACL).

password — specifies a password for users on terminal lines.

logging coredump server

Configure the switch to move (upload) a core dump for an application or kernel crash to an external FTP server.

C9000 Series

Syntax

```
logging coredump server {ipv4-address | ipv6-address} username name password
[type] password
```

Parameters

{*ipv4-address* | *ipv6-address*}	Enter the server IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X).
name	Enter a username to access the target server.
type	Enter the password type: • Enter `0` to enter an unencrypted password. • Enter `7` to enter a password that has already been encrypted using a Type 7 hashing algorithm.
password	Enter a password to access the target server.

Defaults

Core dumps for kernal and application crashes are stored in the local flash of the Control Processor CPU.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0(1.0)	Introduced on the S5000.

Usage Information

The switch supports full core dumps for kernel crashes. The kernel core dump applies to all CPUs and is not enabled by default. To enable full kernel core dumps, enter the `logging coredump` command in global configuration mode. The kernel core dump is copied to the Control Processor (CP) core-dump directory: flash://CORE_DUMP_DIR/f10_*cpu*_*timestamp*.kcore.gz

Where *cpu* specifies a CPU and is one of the following values: **cp** (Control Processor), **cp** (Route Processor), **lp0** (line-card processor 0), **lp1** (line-card processor 1), or **lp2** (line-card processor 2);

timestamp is a text string in the format: *yyyyddmmhhmmss* (YearDayMonthHourMinuteSecond).

Because flash space may be limited, using the `logging coredump server` command ensures your crash (application and kernel) files are uploaded successfully and completely to a server. Only a single core-dump server can be configured. Configuration of a new core dump server over-writes any previously configured server.

NOTE: You must disable logging coredump (`no logging coredump` command) before you configure a new server destination for core dumps.

When you enter the `logging coredump server` command, you are required to enter a password. Use the password of the FTP server where the core files are to be copied. The password can be up to 15 characters; special characters are allowed. After you enter the password, an FTP URL is created with the credentials in the operating system. The CLI monitors core dumps in the unit.

On the switch, when you enable core dumps of application and kernel crashes to be uploaded to an FTP server, only core dumps from the Control Processor are uploaded to the server. Core-dump files from the Route Processor and line-card CPUs are moved to flash memory on the Control Processor CPU and can be accessed by performing an FTP to the Control Processor core-dump directory: flash://CORE_DUMP_DIR/f10_*cpu_timestamp*.kcore.gz

login concurrent-session

Configures the limit of concurrent sessions for each user on console and virtual terminal lines.

Syntax

```
login concurrent-session {limit number-of-sessions | clear—line enable}

no login concurrent-session {limit number-of-sessions | clear—line enable}
```

Parameters

limit *number-of-sessions*	Sets the number of concurrent sessions that any user can have on console and virtual terminal lines. The range is from 1 to 12 (10 VTY lines, one console, and one AUX line).
clear-line enable	Enables you to clear your existing sessions.

Defaults

Not configured. You can use all the available sessions.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.8(0.0)	Introduced on the S4810, S4820, S5000, S6000, S6000-ON, and Z9500.

Usage Information

You must have either the System Administrator or Security Administrator privileges to configure login concurrent-session limit or to enable clear-line.

To limit the number of concurrent sessions that any user can have on console, auxiliary, and virtual terminal lines, use the `login concurrent-session limit` *`number-of-sessions`* command.

If the `login concurrent-session clear-line enable` command is configured, you are provided with an option to clear any of your existing sessions after a successful login authentication. When you reach the maximum concurrent session limit, you can still log in by clearing any of your existing sessions.

Example

The following example shows how to limit the number of concurrent sessions that any user can have to four:

```
DellEMC(conf)# login concurrent-session limit 4
DellEMC(conf)#
```

The following example shows how to use the `login concurrent-session clear-line enable` command.

```
DellEMC(conf)# login concurrent-session clear-line enable
DellEMC(conf)#
```

When you try to log in, the following message appears with all your existing concurrent sessions, providing an option to close any one of the existing sessions:

```
$ telnet 10.11.178.14
Trying 10.11.178.14...
Connected to 10.11.178.14.
Escape character is '^]'.
Login: admin
Password:
Current sessions for user admin:
Line              Location
2  vty 0          10.14.1.97
3  vty 1          10.14.1.97
Clear existing session? [line number/Enter to cancel]:
```

When you try to create more than the permitted number of sessions, the following message appears, prompting you to close one of your existing sessions. Close any of your existing sessions to log in to the system.

```
$ telnet 10.11.178.14
Trying 10.11.178.14...
Connected to 10.11.178.14.
Escape character is '^]'.
Login: admin
Password:
Maximum concurrent sessions for the user reached.
Current sessions for user admin:
Line              Location
2  vty 0          10.14.1.97
3  vty 1          10.14.1.97
4  vty 2          10.14.1.97
5  vty 3          10.14.1.97
Clear existing session? [line number/Enter to cancel]:
```

Related Commands

- login statistics — enable and configure user login statistics on console and virtual terminal lines.
- show login statistics — displays login statistics of users who have used the console or virtual terminal lines to log in to the system.

login statistics

Enable and configure user login statistics on console and virtual terminal lines.

Syntax

```
login statistics {enable | time-period days}

no login statistics {enable | time-period days}
```

Parameters

enable	Enables login statistics for the last 30 days by default.
time-period *days*	Sets the number of days the system stores user login statistics; range is from 1 to 30.

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.8(0.0)	Introduced on the S4810, S4820, S5000, S6000, S6000-ON, and Z9500.

Usage Information

Only the system and security administrators can configure login activity tracking and view the login activity details of other users.

If you enable user login statistics, the system displays the last successful login details of the current user, the details of any failed login attempts by others, and if the current user's permissions have changed since the last login.

If you use the `login statistics time-period days` command to set a custom time period, the system only reports the login statistics during that interval.

NOTE: Login statistics are not applicable for login sessions that do not use authentication on user names. For example, the system does not report login activity for a telnet session that prompts only a password field.

Example

When you log into the system, it displays a message similar to the following:

```
$ telnet 10.11.178.14
Trying 10.11.178.14...
Connected to 10.11.178.14.
```

```
Escape character is '^]'.
Login: admin
Password:
Last successful login: 12:52:01 UTC Tue Mar 22 2016 Line vty0 ( 10.11.178.14 ).
There were 1 unsuccessful login attempt(s) since the last successful login.
There were 1 unsuccessful login attempt(s) for user admin in the last 30
day(s).
There were 1 successful login attempt(s) for user admin in the last 30 day(s).
```

The preceding message shows that the user had previously logged in to the system using the VTY line from 10.11.178.14. It also displays the number of unsuccessful login attempts since the last login and the number of unsuccessful login attempts in the last 30 days.

```
$ telnet 10.11.178.14
Trying 10.11.178.14...
Connected to 10.11.178.14.
Escape character is '^]'.
Login: admin
Password:
Last successful login: 12:52:01 UTC Tue Mar 22 2016 on console
There were 2 unsuccessful login attempt(s) since the last successful login.
There were 3 unsuccessful login attempt(s) for user admin in last 12 day(s).
There were 1 successful login attempt(s) for user admin in the last 30 day(s).
```

The preceding message shows that the user had previously logged in to the system using the console line. It also displays the number of unsuccessful login attempts since the last login and the number of unsuccessful login attempts during a custom time period.

Related Commands

- login concurrent-session — configures the limit of concurrent sessions for each user on console and virtual terminal lines.
- show login statistics — displays login statistics of users who have used the console or virtual terminal lines to log in to the system.

ping

Test connectivity between the system and another device by sending echo requests and waiting for replies.

C9000 Series

Syntax

```
ping [host | ip-address | ipv6-address] [count {number | continuous}]
[datagram-size] [timeout] [source (ip src-ipv4-address) | interface] [tos] [df-
bit (y|n)] [validate-reply(y|n)] [outgoing-interface] [pattern pattern] [sweep-
min-size] [sweep-max-size] [sweep-interval] [ointerface (ip src-ipv4-address) |
interface]
```

Parameters

host	(OPTIONAL) Enter the host name of the devices to which you are testing connectivity.
ip-address	(OPTIONAL) Enter the IPv4 address of the device to which you are testing connectivity. The address must be in the dotted decimal format.
ipv6-address	(OPTIONAL) Enter the IPv6 address, in the x:x:x:x::x format, to which you are testing connectivity. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
count	Enter the number of echo packets to be sent. The default is **5**.

- number: from 1 to 2147483647
- continuous: transmit echo request continuously

datagram size Enter the ICMP datagram size. The range is from 36 to 15360 bytes. The default is **100**.

timeout Enter the interval to wait for an echo reply before timing out. The range is from 0 to 3600 seconds. The default is **2 seconds**.

source Enter the IPv4 or IPv6 source ip address or the source interface. For IPv6 addresses, you may enter global addresses only. Enter the IP address in A.B.C.D format.

- For a Port Channel interface, enter the keyword `port-channel` then a number: The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Tunnel interface, enter the keyword `tunnel` then a number from 1 to 16383.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

tos (IPv4 only) Enter the type of service required. The range is from 0 to 255. The default is **0**.

df-bit (IPv4 only) Enter `Y` or `N` for the “don't fragment” bit in IPv4 header.

- `N`: Do not set the “don't fragment” bit.
- `Y`: Do set “don't fragment” bit

Default is **No**.

validate-reply (IPv4 only) Enter `Y` or `N` for reply validation.

- `N`: Do not validate reply data.
- `Y`: Do validate reply data.

Default is `No`.

outgoing-interface (IPv6 link-local address) Enter the outgoing interface for ping packets to a destination link-local address.

pattern *pattern* (IPv4 only) Enter the IPv4 data pattern. Range: 0-FFFF. Default: **0xABCD**.

sweep-min-size Enter the minimum size of datagram in sweep range. The range is from 52 to 15359 bytes.

sweep-max-size Enter the maximum size of datagram in sweep range. The range is from 53 to 15359 bytes.

sweep-interval Enter the incremental value for sweep size. The range is from 1 to 15308 seconds.

ointerface (IPv4 only) Enter the outgoing interface for multicast packets. Enter the IP address in A.B.C.D format.

- For a Port Channel, enter the keyword `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T. Added support for the `outgoing-interface` option for link-local IPv6 addressing on the S4820T.
8.3.12.0	Added support for the `outgoing-interface` option for link-local IPv6 addressing on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on the ExaScale.
8.4.1.0	IPv6 pinging available on management interface.
8.3.1.0	Introduced extended ping options.
8.2.1.0	Introduced on the E-Series ExaScale (IPv6).
8.1.1.0	Introduced on the E-Series ExaScale (IPv4).
7.9.1.0	Introduced VRF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for IPv6 address on the E-Series.

Usage Information When you enter the `ping` command without specifying an IP/IPv6 address (Extended Ping), you are prompted for a target IP/IPv6 address, a repeat count, a datagram size (up to 1500 bytes), a timeout (in seconds), and for extended commands. For information on ICMP message types, refer to the Usage Information in deny icmp.

The following table provides descriptions for the `ping` command status response symbols displayed in the output.

Symbol	Description
!	Each exclamation point indicates receipt of a reply.
.	Each period indicates the network server timed out while waiting for a reply.
U	A destination unreachable error PDU was received.
Q	Source quench (destination too busy).
M	Could not fragment.
?	Unknown packet type.

Symbol	Description
&	Packet lifetime exceeded.

Example (IPv4)

```
Dell#ping 172.31.1.255

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 172.31.1.255, timeout is 2 seconds:
Reply to request 1 from 172.31.1.208 0 ms
Reply to request 1 from 172.31.1.216 0 ms
Reply to request 1 from 172.31.1.205 16 ms
::
Reply to request 5 from 172.31.1.209 0 ms
Reply to request 5 from 172.31.1.66 0 ms
Reply to request 5 from 172.31.1.87 0 ms
Dell#
```

Example (IPv6)

```
Dell#ping 100::1

Type Ctrl-C to abort.

Sending 5, 100-byte ICMP Echos to 100::1, timeout is 2 seconds:
!!!!!
Success rate is 100.0 percent (5/5), round-trip min/avg/max = 0/0/0 (ms)
Dell#
```

power on

C9000 Series

Syntax `power on`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

reload

Reboot the system.

C9000 Series

Syntax `reload [conditional` *`nvram-cfg-change`* `| pe` *`pe-id`*`]`

From a **PE console**, use `reload` to perform a cold restart.

Parameters

conditional *nvram-cfg-change*	Reload if the condition is true. A configuration change to the nvram requires a switch reload. To reload the switch, select *nvram-cfg-change*.
pe	Reload the RMP, PE unit, or the entire PE stack configured under that PE unit.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added 'conditional' parameter.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information If there is a change in the configuration, the system prompts you to save the new configuration. Or you can save your running configuration with the `copy running-config` command. Use the conditional parameter if any configuration changes made to the nvram, such as stack-group and fanout configurations, must be saved.

To halt a port extender (PE) or an entire PE stack, and perform a cold-restart (from a PE console), use the `reload` command.

send

Send messages to one or all terminal line users.

C9000 Series

Syntax
```
send [*] | [line ] | [console] | [vty]
```

Parameters

*	Enter the asterisk character `*` to send a message to all tty lines.
line	Send a message to a specific line. The range is from 0 to 11.
console	Enter the keyword `console` to send a message to the primary terminal line.
vty	Enter the keyword `vty` to send a message to the virtual terminal.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

Usage Information Messages can contain an unlimited number of lines; however, each line is limited to 255 characters. To move to the next line, use `<CR>`. To send the message use `CTR-Z`; to abort a message, use `CTR-C`.

service timestamps

To debug and log messages, add time stamps. This command adds either the uptime or the current time and date with local time zone time difference included or excluded.

Syntax

```
service timestamps {debug | log} [datetime [localtime] [msec] [show-timezone] [utc] | uptime]
```

To disable timestamping, use the `no service timestamps [debug | log]` command.

Parameters

datetime	(OPTIONAL) Enter the keyword `datetime` to have the current time and date as in local time zone added to the message.
debug	(OPTIONAL) Enter the keyword `debug` to add timestamps to debug messages.
log	(OPTIONAL) Enter the keyword `log` to add timestamps to log messages with severity from 0 to 6.
localtime	(OPTIONAL) Enter the keyword `localtime` to include the local time zone time in the timestamp.
msec	(OPTIONAL) Enter the keyword `msec` to include milliseconds in the timestamp.
show-timezone	(OPTIONAL) Enter the keyword `show-timezone` to include the time zone information in the timestamp.
uptime	(OPTIONAL) Enter the keyword `uptime` to have the timestamp based on time elapsed since system reboot.

utc	(OPTIONAL) Enter the keyword `utc` to include the UTC time format (ignoring local time zone) in the timestamp.

Defaults

- `datetime [localtime]`
- `datetime`

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.5)	Added support for UTC time format.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information If you do not specify parameters and enter service timestamps, it appears as service timestamps debug datetime in the running-configuration.

To view the current options set for the `service timestamps` command, use the `show running-config` command.

From 9.14.1.5 release, the default timestamp display format for the logs is set to local time (`service timestamps log datetime localtime`) instead of `service timestamps log datetime`.

show alarms

View alarms for the system Core, switching core, port modules, fan trays, and power supplies.

C9000 Series

Syntax

```
show alarms [pe pe-id | threshold] all
```

Parameters

pe *pe-id*	(OPTIONAL) Enter the keyword `pe` to display the alarms for port extender (PE). The PE ID range is from 0 to 255.
threshold	(OPTIONAL) Enter the keyword `threshold` to display the temperature thresholds set for the line cards, RPM, SFMs, and PE (when configured).
all	Enter the keyword `all` to display all the alarms corresponding to both the controlling bridge as well as all the PEs checked into it.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced the keyword `all` on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Examples

```
DellEMC#show alarms
--  Minor Alarms  --
Alarm Type                                              Duration
------------------------------------------------------------------------------
No minor alarms

--  Major Alarms  --
Alarm Type                                              Duration
------------------------------------------------------------------------------
```

```
PEM 0 in unit 0 down                                25 sec
PEM 2 in unit 0 down                                6 sec
```

```
DellEMC#show alarm threshold

--  Temperature Limits (deg C)  --
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  linecard0         78         99      84           105      110
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  linecard1         78         99      84           105      110
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  linecard2         78         99      84           105      110
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  linecard3         78         99      84           105      110
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  linecard4         78         99      84           105      110
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  linecard5         78         99      84           105      110
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  linecard6         78         99      84           105      110
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  linecard7         78         99      84           105      110
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  linecard8         78         99      84           105      110
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  RPM0             35         40      43           48       NA
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
  RPM1             35         40      43           48       NA
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
PEid0/Stack0          60         65      72           75       105
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
PEid0/Stack2          60         65      72           75       105
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
PEid0/Stack3          60         65      72           75       105
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
PEid0/Stack4          60         65      72           75       105
-------------------------------------------------------------------------
              Minor Off     Minor   Major Off    Major   Shutdown
PEid0/Stack5          60         65      72           75       105
```

```
DellEMC# show alarms all
    Alarm Type                                              Duration
    ------------------------------------------------------------------------
    Controlling Bridge:
    ==============
    Minor Alarms
            Fan tray 2 of unit 0 has 1 fan(s) failure       21 min, 56 sec
    Major Alarms
            linecard 0 failure                              15 min, 34 sec
            linecard 11 failure                             15 min, 34 sec
    PE ID: 010
    ==========
    Minor Alarms
            PEM 0 in unit 3 removed                         12 hr, 0 min
    Major Alarms
```

```
        No major alarms
PE ID: 020
==========
Minor Alarms
        No minor alarms
Major Alarms
        No major alarms
```

```
DellEMC# show alarms pe all
Alarm Type                                                  Duration
-------------------------------------------------------------------------------
PE ID: 010
==========
Minor Alarms
        PEM 0 in unit 3 removed                              12 hr, 0 min
Major Alarms
        No major alarms
PE ID: 020
==========
Minor Alarms
        No minor alarms
Major Alarms
        No major alarms
```

show asf

View statistics about the Alternate Store and Forward (ASF) packets that are transmitted on the switch line cards.

C9000 Series

Syntax `show asf linecard slot-id`

Parameters

linecard *slot-id*	Enter the slot ID of a line card. The range of slot IDs is from 0 to 2.

Defaults **all**

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series
6.2.1.1	Introduced on the E-Series.

Example

```
Dell#show asf linecard 0
Processor : CP
--------------
Received 100% traffic on TenGigabitEthernet 2/2 Total packets:100
LLC:0, SNAP:0, IP:100, ARP:0, other:0
Unicast:100, Multicast:0, Broadcast:0
Processor : RP1
---------------
Received 62% traffic on TenGigabitEthernet 2/2 Total packets:500
LLC:0, SNAP:0, IP:500, ARP:0, other:0
Unicast:500, Multicast:0, Broadcast:0
Received 37% traffic on TenGigabitEthernet 2/1 Total packets:300
LLC:0, SNAP:0, IP:300, ARP:0, other:0
Unicast:300, Multicast:0, Broadcast:0
Processor : RP2
---------------
No CPU traffic statistics.
Dell#
```

Related Commands debug cpu-traffic-stats — enables CPU traffic statistics for debugging.

show chassis

View the configuration and status of modules in the system. Use this command to determine the chassis mode.

C9000 Series

Syntax

```
show chassis [brief]
```

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to view a summary of the show chassis output.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Example

```
Dell#show chassis brief
Chassis Type  : C9010
Chassis Mode  : 1.0
Chassis MAC   : 34:17:eb:00:20:00

--  Linecard Info  --
LinecardId Type Status   ReqTyp       CurTyp       Version  Ports
```

```
-------------------------------------------------------------------
0   Linecard  online      C9000LC0640  C9000LC0640 9.9(0.0) 24
1   Linecard  not present
2   Linecard  not present C9000LC2410T
3   Linecard  not present
4   Linecard  not present
5   Linecard  online      C9000LC0640  C9000LC0640  9.9(0.0)  24
6   Linecard  online      C9000LC2410G C9000LC2410G 9.9(0.0)  24
7   Linecard  not present
8   Linecard  not present
9   Linecard  not present C9000LC0640
10  Linecard  online      C9000-RPM-2.56T C9000-RPM-2.56T 9.9(0.0) 4
11  Linecard  online      C9000-RPM-2.56T C9000-RPM-2.56T 9.9(0.0) 4

--  Route Processor Modules --
Slot  Status        NxtBoot    Version
-------------------------------------------------------------
  0   active        online     9.9(0.0)
  1   booting

--  Power Supplies  --
Unit  Bay  Status    Type  FanStatus FanSpeed(rpm) Power Usage (W)
-------------------------------------------------------------------
  0   0    down      AC    up        1536          0.0
  0   1    absent
  0   2    up        AC    up        3456          263.5
  0   3    up        AC    up        3440          231.5

Total power:   495.0 W

--  Fan  Status  --
Unit Bay  TrayStatus Fan0 Speed Fan1 Speed Fan2 Speed  Fan3 Speed
-----------------------------------------------------------------
 0   0    up         up   3498  up   3501   up  3464   up   3510
 0   1    up         up   3510  up   3407   up  3501   up   3431
 0   2    up         up   3545  up   3504   up  3440   up   3440

Speed in RPM
```

Related Commands

- show linecard – view the line card status.
- show rpm – view the RPM status.

show command-history

Display a buffered log of all commands all users enter along with a time stamp.

Syntax `show command-history`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.8(0.0P5)	Introduced on the S4048-ON.

Version	Description
9.8(0.0P2)	Introduced on the S3048-ON.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information

One trace log message is generated for each command. No password information is saved to this file. A command-history trace log is saved to a file after failover. Dell EMC Networking TAC analyzes this file to help identify the root cause of it.

The timestamps display format of the `show command-history` output changes based on the `service timestamps log datetime` configuration. The time format can be in uptime, local time or UTC time.

If timestamp is disabled (`no service timestamps log`), the command history time format is shown with timestamp defaults (`service timestamps log datetime localtime`) as in Example 4.

Example

Example 1: Default configuration `service timestamps log datetime` or `service timestamps log datetime localtime`

```
DellEMC#show clock
15:42:42.804 IST Fri May 17 2019
```

```
DellEMC(conf)#service timestamps log datetime
```

Example 2: `service timestamps log datetime utc`

```
DellEMC#show clock
15:47:05.661 IST Fri May 17 2019
```

```
DellEMC(conf)#service timestamps log datetime utc
```

Example 3: `service timestamps log uptime`

```
DellEMC#show clock
15:51:47.534 IST Fri May 17 2019
```

```
DellEMC(conf)#service timestamps log uptime
```

Example 4: `no service timestamps log`

```
DellEMC#show clock
15:55:12.246 IST Fri May 17 2019
```

```
DellEMC(conf)#no service timestamps log
```

```
DellEMC# show command-history
[May 17 15:53:44]: CMD-(CLI):[show logging]by default from console
[May 17 15:53:53]: CMD-(CLI):[show command-history]by default from console
[May 17 15:54:54]: CMD-(CLI):[end]by default from console
[May 17 15:55:00]: CMD-(CLI):[show logging]by default from console
[May 17 15:55:12]: CMD-(CLI):[show clock]by default from console
```

```
[May 17 15:55:22]: CMD-(CLI):[show running-config]by default from console
[May 17 15:55:27]: CMD-(CLI):[show command-history]by default from console
```

show console lp

View the buffered boot-up log of a line card, Route Processor or Control Processor CPU, including background resets, calls, and initialization, on the console.

C9000 Series

Syntax

```
show console {lp slot-id | rp | cp}
```

Parameters

lp*slot-id*	Enter a line-card slot number to view the boot-up log of a line-card (LP) processor. The range of the slot IDs is from 0 to 2.
rp	Enter the `rp` keyword to view the boot-up log for the Route Processor CPU.
cp	Enter the `cp` keyword to view the boot-up log for the Control Processor CPU.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

CAUTION: Use this command only when you are working directly with a technical support representative to troubleshoot a problem. Do not use this command unless a technical support representative instructs you to do so.

show cpu-traffic-stats

View CPU traffic statistics.

C9000 Series

Syntax

```
show cpu-traffic-stats [cp | rp | linecard {slot-id | pe ]
```

Parameters

number	Specify an interface number. The number of interfaces range from 1 to 1568.
all	Enter the keyword `all` to display traffic statistics on all the interfaces.
cp	Enter the keyword `cp` to display traffic statistics on the Control Processor CPU.
rp	Enter the keyword `rp` to display traffic statistics on the Route Processor CPU.
pe	Enter the keyword `pe` to display traffic statistics on the Port Extender.

Defaults

Display CPU traffic statistics for all switch CPUs (Control Processor and Route Processor).

Command Modes

EXEC

Example

```
Dell#show cpu-traffic-stats
```

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series
6.2.1.1	Introduced on the E-Series.

Usage Information

Traffic statistics are sorted on a per-interface basis; the interface receiving the most traffic is displayed first. All CPU and port information is displayed unless a specific port or CPU is specified. Traffic information is displayed for router ports only; not for management interfaces. The traffic statistics are collected only after the `debug cpu-traffic-stats` command is executed; not from the system bootup.

NOTE: After debugging is complete, use the `no debug cpu-traffic-stats` command to shut off traffic statistics collection.

Example

```
Dell#show cpu-traffic-stats
Processor : CP
--------------
```

```
   Received 100% traffic on fortyGigE 2/12   Total packets:8
       LLC:0, SNAP:0, IP:5, ARP:0, other:3
       Unicast:5, Multicast:3, Broadcast:0

Processor : RP
---------------
   Received 100% traffic on fortyGigE 2/12   Total packets:168
       LLC:0, SNAP:0, IP:165, ARP:0, other:3
       Unicast:42, Multicast:126, Broadcast:0
```

Related Commands debug cpu-traffic-stats — enables CPU traffic statistics for debugging.

show cpu-interface-stats

View CPU interface statistics.

C9000 Series

Syntax `show cpu-interface-stats [cp | rp | linecard {slot-id} |all]`

Parameters

cp	Enter the keyword `cp` to display the interface statistics only from the Control Processor.
rp	Enter the keyword `rp` to display the interface statistics only from the Route Processor.
linecard *slot-id*	Enter the `linecard slot-id` parameters to display the interface statistics only from a specified line card. The range of line-card slot IDs is from 0 to 11.
all	Enter the keyword `all` to display the interface statistics from all switch CPUs, including the Control Processor, Route Processor, and line cards.

Defaults Display interface statistics from all switch CPUs.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series
6.2.1.1	Introduced on the E-Series.

Usage Information Traffic statistics are sorted on a per-interface basis; the interface receiving the most traffic is displayed first. All CPU and port information is displayed unless a specific port or CPU is specified. Traffic information is displayed for router ports only; not for management interfaces.

Example

```
Dell#show cpu-traffic-stats cp
-- Partybus ethernet statistics --
Link state           : Up
Recv Interrupts/Polls:         0
Recv Packets         :   2027080    Transmit Packets    :    590000
Recv Desc Error      :         0    Transmit Desc Error :         0
Recv Out of Mem      :         0    Transmit Out of Mem :         0
Recv Upper Layer Full:         0    Transmit Pause Pkts :         0
Recv Other Error     :         0    Transmit Other Error:         0
Recv Restarts        :         0
Recv Restarts Fatal  :         0
-- Dataplane ethernet statistics --

bc pci driver statistics for device:
 rxHandle        :0
 noMhdr          :0
 noMbuf          :0
 noClus          :0
 recvd           :0
 dropped         :0
 recvToNet       :0
 rxError         :0
 rxDatapathErr   :0
 rxPkt(COS0)     :0
 rxPkt(COS1)     :0
 rxPkt(COS2)     :0
 rxPkt(COS3)     :0
 rxPkt(COS4)     :0
 rxPkt(COS5)     :0
 rxPkt(COS6)     :0
 rxPkt(COS7)     :0
 rxPkt(UNIT0)    :0
 rxPkt(UNIT1)    :0
 rxPkt(UNIT2)    :0
 rxPkt(UNIT3)    :0
 transmitted     :0
 txRequested     :0
 noTxDesc        :0
 txError         :0
 txReqTooLarge   :0

 txDatapathErr   :0
 txPkt(COS0)     :0
 txPkt(COS1)     :0
 txPkt(COS2)     :0
 txPkt(COS3)     :0
 txPkt(COS4)     :0
 txPkt(COS5)     :0
 txPkt(COS6)     :0
 txPkt(COS7)     :0
 txPkt(UNIT0)    :0
 txPkt(UNIT1)    :0
 txPkt(UNIT2)    :0
 txPkt(UNIT3)    :0
-- OOB ethernet statistics --
Link state           : N/A
Recv Interrupts/Polls:         0
Recv Packets         :   2269516    Transmit Packets    :    549631
Recv Desc Error      :         0    Transmit Desc Error :         0
Recv Out of Mem      :         0    Transmit Out of Mem :         0
Recv Upper Layer Full:         0    Transmit Pause Pkts :         0
Recv Other Error     :         0    Transmit Other Error:         0
Recv Restarts        :         0
Recv Restarts Fatal  :         0
```

```
-- Thread info ...i .. command output  --
 pthread       state       PRI que state  cntxt sw name     UTIME STIME
 0xb8fbe000   *running     154 ---------f      779 CLI       0.09  0.09
 0xb904e000    running     54 -c----P--f    13163 sSThread  1.01  1.60
 0xb9030000    running     54 ------P--f        6 tSnmpd    0.00  0.00
 0xb902e000    cond_wait   54 -c-C-W---f        1 tSnmpTmr  0.00  0.00
 0xb90ac000    running     54 ------P--f       88 auxd      0.00  0.00
 0xb9125000    select_wait 154 ----RW---f     2455 CLIInit   0.31  0.43
 0xb92f0000    select_wait 54 ----RW---f       86 DHCLIENT  0.01  0.00
 0xb931a000    select_wait 54 ----RW---f        1 cms       0.00  0.00
 0xb93a3000    select_wait 54 ----RW---f     6672 portmirr  0.24  0.25
 0xb93bd000    select_wait 54 ----RW---f        2 cfgDataS  0.00  0.00
 0xb93d1000    select_wait 54 ----RW---f        2 sysCompM  0.00  0.00
 0xb9470000    select_wait 54 ----RW---f   166043 statMgr   7.09  6.28
 0xb94c8000    running     54 ------P--f  1579998 sflCp    37.86 43.13
 0xb9560000    running     54 ------P--f    21857 snmp      0.95  1.69
 0xb99e0000    running     54 ------P--f       25 usm       0.00  0.02
 0xb957f000    running     54 ------P--f    72691 dpi_daem  4.50  4.16
 0xb9594000    select_wait 54 ----RW---f        2 dpi       0.00  0.00
 0xb95a8000    select_wait 54 ----RW---f   376512 diagmgr   3.80  6.18

-- netstat -i command output  --
Name  Mtu   Network       Address            Ipkts Ierrs    Opkts Oerrs Colls
Drops
bc0   1500          00:00:00:00:00:00        0     0        0     0     0     0
mul0  1500          00:00:00:00:00:00        0     0        0     0     0     0
wm0   1500          74:86:7a:ff:6f:24  2240632    17   608097     0     0     0
wm1   9710          74:86:7a:ff:6e:a0        0     0        0     0     0     0
lo0   33192                                212314     0   212314     0     0     0
lo0   33192 ::1/128       ::1             212314     0   212314     0     0     0
lo0   33192 127.0.0/24    127.0.0.1       212314     0   212314     0     0     0
backp 1500          74:86:7a:ff:6f:24  2027232     0   590069     0     0     0
backp 1500  127.10.10/24  RPM0-CP        2027232     0   590069     0     0     0
backp 1500  127.10.10.43/ LC-3           2027232     0   590069     0     0     0
rcpu0 9000          74:86:7a:ff:6e:a0        0     0        0     0     0     0
cop0  1500          00:00:00:00:00:00        0     0        0     0     0     0
ifdbg 2000                                   0     0        0     0     0     0
ifarp 2000                                   0     0        0     0     0     0
ificm 2000                                   0     0        0     0     0     0
ifdbg 2000                                   0     0        0     0     0     0
ifacl 2000                                   0     0        0     0     0     0
if6db 2000                                   0     0        0     0     0     0
if6db 2000                                   0
```

Related Commands debug cpu-traffic-stats — enables CPU traffic statistics for debugging.

show debugging

View a list of all enabled debugging processes.

C9000 Series

Syntax `show debugging`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series
E-Series	Original command.

Example

```
Dell#show debugging
Generic IP:
  IP packet debugging is on for
    ManagementEthernet 0/0
    Port-channel 1-2
    Port-channel 5
    TenGigabitEthernet 0/0-3,5-6,10-11,20
    TenGigabitEthernet 1/0-1,5-6,10-11,15,17,19,21
  ICMP packet debugging is on for
    TenGigabitEthernet 1/0,2,4,6,8,10,12,14,16
  DHCP Server:
    DHCP server packet debugging on
Dell#
```

show environment

View system component status (for example, temperature or voltage).

Syntax `show environment [all | fan | pem | stack-unit unit-id ]`

Parameters

all	Enter the keyword `all` to view all components.
fan	Enter the keyword `fan` to view information on the fans. The output of this command is chassis-dependent.
pem	Enter the keyword `pem` to view only information on power entry modules.
stack-unit *unit-id*	Enter the keywords `stack-unit` then the unit-id to display information on a specific stack member.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(2.1P1)	The CLI has been enhanced to show the power, average power and average power start time.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	The output of the `show environment fan` command for the S Series is changed to display fan speeds instead of showing the fan status as up or down.

Usage Information

The following example shows the output of the `show environment` command.

Example (all)

This output is applicable for the C9000 platform.

```
DellEMC#show env
--  Fan  Status  --
Unit Bay   TrayStatus  Fan1    Speed
-------------------------------------
1    1     up          up      10780
1    2     up          up      10780
1    3     up          up      10780
1    4     up          up      10780
1    5     up          up      10780

Speed in RPM

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus   FanSpeed   Power  AvgPower  AvgPowerStartTime
-------------------------------------------------------------------------------
  0       0        up           AC      up          3104        174       175      05/26/2017-03:33
  0       1    absent
  0       2        up           AC      up          3104        174       175      05/26/2017-03:33
  0       3    absent
Total power:   348.0 W

-- Unit Environment Status  --
Unit  Status        Temp   Voltage
-----------------------------------
* 1   online        28C    ok

* Management Unit

--  Thermal Sensor Readings (deg C)  --
Unit  Sensor-CPU  Sensor-MAC  Sensor-Left  Sensor-Right  Sensor-QSFP  Sensor-DCFAN  Sensor-BCM
-----------------------------------------------------------------------------------------------
  1          25          28          25          22          26          23          36
```

Example (System Power Log)

This output is applicable for the C1048P, N20xx, and N30xx series port-extenders.

```
DellEMC# show env
```

```
--  Fan  Status  --
Unit Bay   TrayStatus  Fan1    Speed   Fan2    Speed
-----------------------------------------------------
 1     1   up          up      9056    up      9056
 1     2   up          up      9037    up      9037

Speed in RPM

--  Power Supplies  --
Unit   Bay   Status   Type    FanStatus  FanSpeed(rpm)
-----------------------------------------------------
  1     1    up       AC      up         NA
  1     2    up       AC      up         NA

Unit   TotalPower   AvgPower   AvgPowerStartTime
-----------------------------------------------
1      30            26          05/25/2017-19:18
```

show inventory

Display the switch type, components (including media), and Dell Networking OS version, including hardware identification numbers and configured protocols.

C9000 Series

Syntax

`show inventory [media [slot-id | pe pe-id [stack-unit unit-number]]| pe pe-id]`

From a **PE console**, use `show inventory [media]` to view the PE inventory information.

Parameters

media *slot-id*	(OPTIONAL) Enter the keyword `media` to display pluggable media inventory for a specified line-card slot. Valid slot IDs are from 0 to 2.
pe *pe-id*	(OPTIONAL) Enter the keyword `pe` to display port extender (PE) inventory for a specified PE ID. Range is from 0 to 255.

NOTE: The pe option is only available when the extended bridge feature is enabled.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9 (0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.4	Output expanded to include Piece Part ID (PPID) and eSR4 optics.

Version	Description
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced this version of the command for S-Series. S-Series output differs from E-Series.

Usage Information

Use the `show inventory` command to display information about installed pluggable media (QSFP, SFP) on a line card. If no optics are installed in the fiber ports, the output displays *Media not present or accessible*.

When feature extender bridge is enabled on C9000, the **pe** option displays port extender inventory for a specified PE.

Example

```
Dell#show inventory
Chassis Type           : C9010
Chassis Mode           : 1.0
Software Version       : 1-0(0-4079)

Slot Type Serial Number  Part Number  Rev  Piece Part ID           Rev  Svc Tag ExprsSvc Code
  0       C9010            NA     0500WH       X00  CN-0500WH-77931-4A7-0009 X00  16DQG02  256 264 819 4
  0       C9000LC2410G             04D4GD       X00  CN-04D4GD-77931-4A8-0013 X00  16NQG02  257 944 435 4
  1       C9000LC2410G             04D4GD       X00  CN-04D4GD-77931-4A7-0015 X00  16HTG02  256 950 662 6
  2       C9000LC2410G             04D4GD       X00  CN-04D4GD-77931-4A7-0011 X00  16GTG02  256 782 701 0
  3       C9000LC2410T             0KFHFG       X00  CN-0KFHFG-77931-4A6-0004 X00  15GQG02  250 722 086 6
  4       C9000LC2410T             0KFHFG       X00  CN-0KFHFG-77931-4A5-0013 X00  15BRG02  249 886 944 2
  5       C9000LC2410T             0KFHFG       X00  CN-0KFHFG-77931-4A6-0006 X00  15GSG02  250 731 417 8
  6       C9000LC0640              0CYFF2       X00  CN-0CYFF2-77931-4A6-0012 X00  15VQG02  253 241 510 6
  7       C9000LC0640              0CYFF2       X00  CN-0CYFF2-77931-4A6-0030 X00  161RG02  254 253 945 8
  8       C9000LC0640              0CYFF2       X00  CN-0CYFF2-77931-4A6-0017 X00  15WSG02  253 418 803 4
* 0       C9000-RPM-2.56T  NA     0CKKCP       X00  CN-0CKKCP-77931-4A6-0005 X00  168SG02  255 434 342 6
  1       C9000-RPM-2.56T  NA     0CKKCP       X00  CN-0CKKCP-77931-49U-0026 X00  14XQG02  247 530 816 2
  0       C9000-PWR-AC-R   NA     05PDWGX02    X02  CN-05PDWG-17972-48M-00BY N/A  N/A      0
  1       C9000-PWR-AC-R   NA     05PDWGX02    X02  CN-05PDWG-17972-48M-00CQ N/A  N/A      0
  2       C9000-PWR-AC-R   NA     05PDWGX02    X02  CN-05PDWG-17972-48M-0087 N/A  N/A      0
  3       C9000-PWR-AC-R   NA     05PDWGX02    X02  CN-05PDWG-17972-48M-00CD N/A  N/A      0
  0       C9000-FAN        NA     09H0H0       X00  CN-09H0H0-77931-4A8-0023 X00  NA       NA
  1       C9000-FAN        NA     09H0H0       X00  CN-09H0H0-77931-4A8-0028 X00  NA       NA
  2       C9000-FAN        NA     09H0H0       X00  CN-09H0H0-77931-4A8-0012 X00  NA       NA

 * - Primary RPM


Software Protocol Configured
----------------------------
 Extended Bridge
```

Example (PE)

```
Dell#show inventory pe 4
System Type : C1048P
System Mode : 1.0
Software Version : 1-0(0-4784)
Unit Type          Serial Number Part Number Rev Piece Part ID
--   -------------  ------------ ----------- --- ------------
* 0  C1048P-01-1G-48 NA          7590009701  001  US-0F14T0-77951-3AG-000A
  0  C1048P-PWR-AC   NA          001ABCD001  00A  US-001YHN-17972-38N-007A
  0  C1048P-PWR-DC                            N/A
  0  C1048P-FAN                               N/A
* 0  usbflash:                      -          N/A

* - Management Unit
```

Example (PE Console)

```
Dell#show inventory
System Type            : C1048P
System Mode            : 1.0
Software Version       : 1-0(0-4092)

Unit Type      Serial Number Part Number  Rev  Piece Part ID           Rev  Svc Tag
Exprs Svc Code
---- --------  ------------- -----------  ---- ----------------------- ---- -------
--------------
* 1  C1048P-01-1G-48    NA     7590009701 001  US-0F14T0-77951-3AG-000A 01   NA       NA
  1  C1048P-PWR-AC      NA     001ABCD001 00A  US-001YHN-17972-38N-007A 001  NA       NA
  1  C1048P-FAN         N/A                  N/A                             N/A
N/A

 * - Management Unit


Software Protocol Configured
```

```
---------------------------
  LLDP
```

Related Commands

- show interfaces — displays the interface configuration.
- show interfaces transceiver — displays the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show linecard

Display the linecard(s) status.

C9000 Series

Syntax

```
show linecard [slot-id [brief] | all]
```

Parameters

slot-id	(OPTIONAL) Enter a slot ID to view information on the line card in that slot. For the C9010, the range is from 0 to 11. For the C-Series, the range is 0 to 7. For the E-Series, the range is 0 to 13 on the E1200, 0 to 6 on the E600, and 0 to 5 on the E300.
all	(OPTIONAL) Enter the keyword `all` to view a table with information on all present line cards
brief	(OPTIONAL) Enter the keyword `brief` to view an abbreviated list of line card information.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

`show linecard output` Field	Description
Line card	Displays the line card slot number (only listed in the `show linecard all` command output).
Status	Displays the line card's status.
Next Boot	Displays whether the line card is to be brought online at the next system reload.
Required Type	Displays the line card type configured for the slot. The Required Type and Current Type must match. If they do not match, use the `linecard` command to reconfigure the line card type.

show linecard output Field	Description
Current Type	Displays the line card type installed in the slot. The Required Type and Current Type must match. If they do not match, use the `linecard` command to reconfigure the line card type.
Hardware Rev	Displays the chipset revision.
Num Ports	Displays the number of ports in the line card.
Up Time	Displays the number of hours and minutes the card is online.
Dell Networking OS Version	Displays the operating software version.
Jumbo Capable	Displays Yes or No indicating if the line card can support Jumbo frames.
Boot Flash Ver	Displays the two possible Bootflash versions. The [Booted] keyword next to the version states which version was used at system boot.
Memory Size	List the memory of the line card processor.
Temperature	Displays the temperature of the line card. Minor alarm status if the temperature is over 65º C.
Power Status	Lists the type of power modules used in the chassis: • AC = AC power supply • DC = DC Power Entry Module (PEM)
Voltage	Displays OK if the line voltage is within range.
Serial Number	Displays the line card serial number.
Part Num	Displays the line card part number.
Vendor ID	Displays an internal code, which specifies the manufacturing vendor.
Date Code	Displays the line card's manufacturing date.

Example (C9010)

```
Dell#show linecard 0

--  Linecard 0 --
Status                     : online
Next Boot                  : online
Required Type              : C9000LC0640 - 6-port TE/FG
Current Type               : C9000LC0640 - 6-port TE/FG
Hardware Rev               : 4.0
Num Ports                  : 24
Up Time                    : 2 hr, 47 min
Dell Networking OS Version : 9.9(0.0)
Jumbo Capable              : yes
POE Capable                : Not supported
Max Required Power         : 153
Boot Flash                 : 3.3.1.16
Boot Selector              : 3.3.0.1
Memory Size                : 2127654912 bytes
Serial Number              :
Part Number                : 0CYFF2     Rev X00
Vendor Id                  :
Date Code                  :
Country Code               :
Piece Part ID              : CN-0CYFF2-77931-452-0008
PPID Revision              : X00
Service Tag                : 11VRG02
```

```
Expr Svc Code              : 229 059 705 8
Auto Reboot                : disabled
Last Restart               : powered-on
Burned In MAC              : 34:17:eb:00:20:00
No Of MACs                 : 3
```

Example (E-Series)

```
Dell#show linecard 11
-- Line card 11 --
Status        : online
Next Boot     : online
Required Type : E48PF - 48-port GE line card with SFP optics
(EF)
Current Type  : E48PF - 48-port GE line card with SFP optics
(EF)
Hardware Rev  : Base - 1.0 PP0 - n/a PP1 - n/a
Num Ports     : 48
Up Time       : 12 hr, 37 min
FTOS Version  : 6.2.1.x
Jumbo Capable : yes
Boot Flash    : A: 2.0.3.4 B: 2.0.3.4 [booted]
Memory Size   : 268435456 bytes
Temperature   : 49C
Power Status  : PEM0: absent or down PEM1: up
Voltage       : ok
Serial Number :
Part Number   : Rev
Vendor Id     :
Date Code     :
Country Code  :
Dell#
```

Example (C-Series)

```
Dell#show linecard 11
-- Line card 11 --
Status        : online
Next Boot     : online
Required Type : E48PF - 48-port GE line card with SFP optics
(EF)
Current Type  : E48PF - 48-port GE line card with SFP optics
(EF)
Hardware Rev  : Base - 1.0 PP0 - n/a PP1 - n/a
Num Ports     : 48
Up Time       : 12 hr, 37 min
FTOS Version  : 6.2.1.x
Jumbo Capable : yes
Boot Flash    : A: 2.0.3.4 B: 2.0.3.4 [booted]
Memory Size   : 268435456 bytes
Temperature   : 49C
Power Status  : PEM0: absent or down PEM1: up
Voltage       : ok
Serial Number :
Part Number   : Rev
Vendor Id     :
Date Code     :
Country Code  :
Dell#
```

Example (brief)

```
Dell#show linecard 11 brief
-- Line card 11 --
Status        : online
Next Boot     : online
Required Type : E48PF - 48-port GE line card with SFP optics (EF)
Current Type  : E48PF - 48-port GE line card with SFP optics (EF)
Hardware Rev  : Base - 1.0 PP0 - n/a PP1 - n/a
Num Ports     : 48
Up Time       : 11 hr, 24 min
FTOS Version  : 6.1.1.0
```

```
Jumbo Capable : yes
Dell#
```

Related Commands

- show interfaces linecard — displays information on all interfaces on a specific line card.
- show chassis — view information on all elements of the system.
- show rpm — view information on the RPM.

show login statistics

Displays login statistics of users who have used the console or virtual terminal lines to log in to the system.

Syntax

```
show login statistics [all | [[successful-attempts | unsuccessful-attempts]
[user login-id] [time-period days]] | user login-id]
```

Parameters

all	(Optional)Displays the login statistics of all users in the last 30 days or the custom defined time period.
time-period *days*	(Optional)Displays the number of failed login attempts by the current user in the specified period.
successful-attempts	(Optional)Displays the number of successful login attempts by the current user in the last 30 days or the custom defined time period
unsuccessful-attempts	(Optional)Displays the number of failed login attempts by the current user in the last 30 days or the custom defined time period.
user *login-id*	(Optional)Displays the login statistics of a specific user in the last 30 days or the custom defined time period. When you use it with the `unsuccessful-attempts` keyword, the system displays the number of failed login attempts by a specific user in the last 30 days or the custom defined time period

Defaults None

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced the `successful-attempts` keyword.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.

Version	Description
9.8(0.0)	Introduced on the S4810, S4820, S5000, S6000, S6000-ON, and Z9500.

Usage Information

To view the successful and failed login details of the current user in the last 30 days or the custom defined period, use the `show login statistics` command.

To view the successful and failed login details of all users in the last 30 days or the custom defined period, use the `show login statistics all` command. You can use this command only if you have system or security administrator rights.

To view the successful and failed login details of a specific user in the last 30 days or the custom defined time period, use the `show login statistics user` *`user-id`* command. If you have system or security administrator rights, you can view the login statistics of other users. If you do not have system or security administrator rights, you can view your login statistics but not the login statistics of others.

NOTE: By default, these commands display the details for the last 30 days. If you set a custom-defined time period for login statistics using the `login statistics time-period` *`days`* command, these commands display details only for that period.

Example

The following is sample output of the `show login statistics` command.

```
DellEMC#show login statistics

------------------------------------------------------------------
User: admin
Last login time: 12:52:01 UTC Tue Mar 22 2016
Last login location: Line vty0 ( 10.16.127.143 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 30 day(s): 0
Successful login attempt(s) in last 30 day(s): 1
------------------------------------------------------------------
```

The following is sample output of the `show login statistics all` command.

```
DellEMC#show login statistics all

------------------------------------------------------------------
User: admin
Last login time: 08:54:28 UTC Wed Mar 23 2016
Last login location: Line vty0 ( 10.16.127.145 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 30 day(s): 3
Successful login attempt(s) in last 30 day(s): 4
------------------------------------------------------------------

------------------------------------------------------------------
User: admin1
Last login time: 12:49:19 UTC Tue Mar 22 2016
Last login location: Line vty0 ( 10.16.127.145 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 30 day(s): 3
Successful login attempt(s) in last 30 day(s): 2
------------------------------------------------------------------

------------------------------------------------------------------
User: admin2
Last login time: 12:49:27 UTC Tue Mar 22 2016
Last login location: Line vty0 ( 10.16.127.145 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 30 day(s): 3
Successful login attempt(s) in last 30 day(s): 2
------------------------------------------------------------------
```

```
------------------------------------------------------------------
User: admin3
Last login time: 13:18:42 UTC Tue Mar 22 2016
Last login location: Line vty0 ( 10.16.127.145 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 30 day(s): 3
Successful login attempt(s) in last 30 day(s): 2
```

The following is sample output of the `show login statistics user user-id` command.

```
DellEMC# show login statistics user admin

------------------------------------------------------------------
User: admin
Last login time: 12:52:01 UTC Tue Mar 22 2016
Last login location: Line vty0 ( 10.16.127.143 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 30 day(s): 0
Successful login attempt(s) in last 30 day(s): 1
------------------------------------------------------------------
```

The following is sample output of the `show login statistics unsuccessful-attempts` command.

```
DellEMC#show login statistics unsuccessful-attempts
There were 3 unsuccessful login attempt(s) for user admin in last 30 day(s).
```

The following is sample output of the `show login statistics unsuccessful-attempts time-period days` command.

```
DellEMC# show login statistics unsuccessful-attempts time-period 15
There were 0 unsuccessful login attempt(s) for user admin in last 15 day(s).
```

The following is sample output of the `show login statistics unsuccessful-attempts user login-id` command.

```
DellEMC# show login statistics unsuccessful-attempts user admin
There were 3 unsuccessful login attempt(s) for user admin in last 12 day(s).
```

The following is sample output of the `show login statistics successful-attempts` command.

```
DellEMC#show login statistics successful-attempts
There were 4 successful login attempt(s) for user admin in last 30 day(s).
```

Related Commands

- login statistics — enable and configure user login statistics on console and virtual terminal lines.
- login concurrent-session — configures the limit of concurrent sessions for each user on console and virtual terminal lines.

show memory

View current memory usage on the system.

C9000 Series

Syntax `show memory [cp | lp {slot-id | pe [pe-id stack-unit unit-number] | rp}]`

Parameters

cp Enter the keyword `cp` to display memory usage on the Control Processor CPU.

rp	Enter the keyword `rp` to display memory usage on the Route Processor CPU.
lp *slot-id*	Enter the slot ID of the line card for which you want to display memory usage. The slot ID range is from 0 to 11.
pe *pe-id*	Enter the keyword `pe` then the port extender (PE) ID to display memory usage on the PE. The PE ID range is from 0 to 255. **NOTE: The pe option is only available when the extended bridge feature is enabled.**
stack-unit *unit-number*	Enter the keyword `stack-unit` then the stack unit number. Range is from 0 to 7.

Command Modes

- EXEC
- EXEC Privilege

Defaults

Display memory usage on all switch CPUs (Control Processor, Route Processor, and line cards).

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

The output for `show memory` displays the memory usage of the line-card processor (LP) part (sysdlp) of the system. The sysdlp is an aggregate task that handles all the tasks running on the LP.

The total counter size in `show memory` and `show processes memory` differs based on which OS processes are counted.

- In the `show memory` output, the memory size is equal to the size of the application processes.
- In the `show processes memory` output, the memory size is equal to the size of the application processes plus the size of the system processes.

Examples

```
Dell#show memory

     Statistics On  CP Processor
     ============================
   Total(b)       Used(b)        Free(b)       Lowest(b)       Largest(b)
  3203928064        6953130    3196974934    3196941986    3196974934
     Statistics On  RP Processor
     ============================
   Total(b)       Used(b)        Free(b)       Lowest(b)       Largest(b)
  3203928064       17806442    3186121622    3186088674    3186121622
```

```
Dell#show memory cp
   Total(b)      Used(b)       Free(b)      Lowest(b)      Largest(b)
  3203928064       6953130    3196974934   3196974934   3196974934


Dell#show memory rp
   Total(b)      Used(b)       Free(b)      Lowest(b)      Largest(b)
  3203928064      17174702    3186753362   3186753362   3186753362

Dell#show memory lp 2
   Total(b)      Used(b)       Free(b)      Lowest(b)      Largest(b)
  3203928064       8555410    3195372654   3195372654   3195372654
```

"Lowest" displays the memory usage the system went to in the lifetime of the system. Indirectly, it indicates the maximum usage in the lifetime of the system: Total minus Lowest.

"Largest" displays the current largest available. This relates to the block size and is not related to the amount of memory on the system.

Example (PE)

```
Dell# show memory pe 4 stack-unit 0
   Total(b)      Used(b)       Free(b)      Lowest(b)      Largest(b)
  1073741824     829850       1072911974   1072829154      1072911974
```

show processes cpu

View information on CPU usage for processes running in the system.

C9000 Series

Syntax

```
show processes cpu [cp number of tasks | details ]| lp {slot-id
number of tasks | all | cp-lp | summary} | pe { pe-id stack-unit unit number
| all | [number of tasks]}| rp {[number of tasks | details]} summary
```

Parameters

cp	Enter the keyword `cp` to view CPU usage for the Control Processor.
lp	Enter the keyword `lp` to view CPU usage for the Line Processor.
rp	Enter the keyword `rp` to view CPU usage for the Route Processor.
pe *pe-id*	Enter the keyword `pe` and the port extender (PE) ID. Range is from 0 to 255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the stack unit number. Range is from 0 to 7.
all	Enter the keyword `all` to display usage information for all switch CPUs: control processor, route processor, and linecards.
summary	Enter the keyword `summary` to view a summary of CPU usage.
details	Enter the keyword `details` to view detailed information about CPU usage.

Command Modes

- EXEC

- EXEC Privilege

Defaults

Display detailed information on CPU usage for all switch CPUs (control processor, route processor, and linecards).

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.

Usage Information

In a dual homing setup, you can use this command only from the primary VLT peer.

The following examples display CPU usage information for the control processor (CP), route procesor (RP), and the port extender (PE).

Example show processes cpu cp

```
Dell#show processes cpu cp

CPUID       5sec       1min       5min
-------- ---------- ---------- ----------
CORE  0     0.59       1.18       0.00
CORE  2     0.20       0.44       0.00
Overall     0.40       0.81       0.00


CPU utilization of sysdlp for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID        Runtime(ms)  Invoked   uSecs    5Sec   1Min    5Min TTY       Process
0x000001ef      181290    18129   10000   0.20%   0.20%   0.20%  0        sysdlp
0x0000020c      182530    18253   10000   0.10%   0.17%   0.23%  0          sysd
0x00000000      171610    17161   10000   0.05%   0.16%   0.25%  0        system
0x0000013f        7550      755   10000   0.05%   0.02%   0.01%  0         dot1x
0x0000027c       12300     1230   10000   0.05%   0.02%   0.01%  0         sflow
0x0000020f        5210      521   10000   0.00%   0.02%   0.01%  0   f10dhclient
0x00000137        5160      516   10000   0.00%   0.02%   0.00%  0        ndpmul
0x000002f1        7730      773   10000   0.00%   0.02%   0.01%  0     Dhcpv6Rly
0x00000073        4920      492   10000   0.00%   0.02%   0.00%  0      ipSecMgr
0x00000291        5500      550   10000   0.00%   0.02%   0.01%  0         ssMgr
0x00000244        5370      537   10000   0.00%   0.01%   0.00%  0           ntp
0x00000265        5180      518   10000   0.00%   0.01%   0.00%  0  f10dhcpv4rly
0x000002bd        4950      495   10000   0.00%   0.01%   0.00%  0          otm
0x00000099       15360     1536   10000   0.00%   0.01%   0.02%  0          brm
0x000002ce        7220      722   10000   0.00%   0.01%   0.03%  0        clish
0x000000f5        5000      500   10000   0.00%   0.01%   0.00%  0   vlthrtbtrly
0x000000e3        5480      548   10000   0.00%   0.01%   0.00%  0       tnlmgr
0x00000249        6620      662   10000   0.00%   0.01%   0.01%  0          ipm
0x00000228       12430     1243   10000   0.00%   0.00%   0.02%  0       radius
0x000002bb        8380      838   10000   0.00%   0.00%   0.01%  0        ofmgr
0x000001f8         640       64   10000   0.00%   0.00%   0.00%  0       sysmon
0x000001f4        1090      109   10000   0.00%   0.00%   0.00%  0       sysmon
0x000000df        3140      314   10000   0.00%   0.00%   0.00%  0    flashmntr
0x000000d7           0        0       0   0.00%   0.00%   0.00%  0        inetd
0x00000095         750       75   10000   0.00%   0.00%   0.00%  0         rngd
0x00000079          40        4   10000   0.00%   0.00%   0.00%  0           sh
0x00000043          10        1   10000   0.00%   0.00%   0.00%  0           sh
0x00000013         610       61   10000   0.00%   0.00%   0.00%  0    mount_mfs
0x00000002          40        4   10000   0.00%   0.00%   0.00%  0           sh
0x00000001           0        0       0   0.00%   0.00%   0.00%  0         init
0x00000327         100       10   10000   0.00%   0.00%   0.00%  0       ssCron
0x0000029d          10        1   10000   0.00%   0.00%   0.00%  0           sh
0x00000250          10        1   10000   0.00%   0.00%   0.00%  0           sh
0x0000024a         190       19   10000   0.00%   0.00%   0.00%  0        login
```

Example show processes rp

```
Dell#sho processes cpu rp

CPUID         5sec            1min            5min
-------- ----------------- -------------- -----------
CORE  0       0.20            0.00            0.00
CORE  2       0.00            0.00            0.00
Overall       0.10            0.00            0.00


CPU utilization of sysdlp for five seconds:0%/0%; one minute: 0%;five minutes: 0%
PID       Runtime(ms)   Invoked  uSecs    5Sec  1Min    5Min TTY  Process
0x000001e6    28780     2878     10000   0.10%  0.05%  0.05%  0   lacp
0x00000197     2250      225     10000   0.00%  0.01%  0.00%  0   sysd
0x0000019b     1730      173     10000   0.00%  0.01%  0.01%  0   sysmon
0x00000127      960       96     10000   0.00%  0.00%  0.00%  0   xstp
0x00000152     1660      166     10000   0.00%  0.00%  0.00%  0   l2mgr
0x000001ed     1010      101     10000   0.00%  0.00%  0.00%  0   arpm
0x000001b4     1070      107     10000   0.00%  0.00%  0.00%  0   l3Mgr
0x0000022b     1410      141     10000   0.00%  0.00%  0.00%  0   vrrp
0x00000061     1260      126     10000   0.00%  0.00%  0.00%  0   ipm1
0x000001cb     1190      119     10000   0.00%  0.00%  0.00%  0   rtm
0x000001c5     1160      116     10000   0.00%  0.00%  0.00%  0   acl
0x000001f5     1280      128     10000   0.00%  0.00%  0.00%  0   mrtm
0x000000a3      940       94     10000   0.00%  0.00%  0.00%  0   igmp
0x000001ef      940       94     10000   0.00%  0.00%  0.00%  0   ndpm
0x0000018f      940       94     10000   0.00%  0.00%  0.00%  0   dsm
0x000001c9     1770      177     10000   0.00%  0.00%  0.00%  0   frrp
0x000001d0      900       90     10000   0.00%  0.00%  0.00%  0   rip
0x0000020d      900       90     10000   0.00%  0.00%  0.00%  0   mlagmgr
0x000001a9     1010      101     10000   0.00%  0.00%  0.00%  0   l2pm
0x00000225     1280      128     10000   0.00%  0.00%  0.00%  0   pim
0x0000019e        0        0         0   0.00%  0.00%  0.00%  0   sh
0x000000c7      170       17     10000   0.00%  0.00%  0.00%  0  flashmntr
0x000000bc        0        0         0   0.00%  0.00%  0.00%  0   inetd
0x0000007a      580       58     10000   0.00%  0.00%  0.00%  0   rngd
0x00000013      260       26     10000   0.00%  0.00%  0.00%  0  mount_mfs
0x00000002        0        0         0   0.00%  0.00%  0.00%  0   sh
0x00000001        0        0         0   0.00%  0.00%  0.00%  0   init
0x00000000     5640      564     10000   0.00%  0.00%  0.00%  0   system
```

Example show processes cpu pe

```
Dell#show processes cpu pe 1 stack-unit 3

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID       Runtime(ms)Invoked   uSecs    5Sec   1Min    5Min TTY         Process
0x4ba48020       20       2    10000   0.00%  0.00%   0.00%   0          POEAgt
0x4bb1f020      590      59    10000   0.00%  0.00%   0.00%   0         diagagt
0x4bb09020        0       0        0   0.00%  0.00%   0.00%   0        debugagt
0x4baf5020       10       1    10000   0.00%  0.00%   0.00%   0       F10StkMgr
0x4badf020     1090     109    10000   0.00%  0.00%   0.00%   0          envmgr
0x4bac9020     1210     121    10000   0.00%  0.00%   0.00%   0           lcMgr
0x4ba2f020     1210     121    10000   0.00%  0.00%   0.00%   0             dla
0x4ba0c020      340      34    10000   0.00%  0.00%   0.00%   0       sysAdmTsk
0x4b9f7020     3520     352    10000   0.00%  0.00%   0.00%   0        timerMgr
0x4b9e0020      220      22    10000   0.00%  0.00%   0.00%   0              PM
0x4b9c8020     8060     806    10000   0.00%  0.00%   0.00%   0              KP
0x4b9b2020        0       0        0   0.00%  0.00%   0.00%   0           evagt
0x4b995020      220      22    10000   0.00%  0.00%   0.00%   0             ipc
0x4b981020      100      10    10000   0.00%  0.00%   0.00%   0       sysReaper
0x4b927020       30       3    10000   0.00%  0.00%   0.00%   0             tme
0x4b912020        0       0        0   0.00%  0.00%   0.00%   0    ttraceIpFlow
0x4b8fc020        0       0        0   0.00%  0.00%   0.00%   0         isrTask
0x4af6f020        0       0        0   0.00%  0.00%   0.00%   0            tDDB
0x4af6e020       20       2    10000   0.00%  0.00%   0.00%   0              GC
0x4af6a020       20       2    10000   0.00%  0.00%   0.00%   0 linkscan_user_t
0x4af4e020        0       0        0   0.00%  0.00%   0.00%   0 bshell_reaper_t
0x4ab97020        0       0        0   0.00%  0.00%   0.00%   0         tSysLog
0x4ab87020      500      50    10000   0.00%  0.00%   0.00%   0      tTimerTask
0x4ab86020    15330    1533    10000   0.00%  0.00%   0.02%   0        tExcTask
0x4ab57020       20       2    10000   0.00%  0.00%   0.00%   0        tLogTask
0x4ab36020     8940     894    10000   0.00%  0.00%   0.00%   0        tUsrRoot
0x4068f020      100      10    10000   0.00%  0.00%   0.00%   0            main
0x4bea8020        0       0        0   0.00%  0.00%   0.00%   0     poePortScan
0x4c60c020      820      82    10000   0.00%  0.00%   0.00%   0      V6RadAgent
0x4c5f3020      200      20    10000   0.00%  0.00%   0.00%   0         brAgent
0x4c5dd020        0       0        0   0.00%  0.00%   0.00%   0 nvProcessMwpAck
0x4c5c7020       30       3    10000   0.00%  0.00%   0.00%   0         IpAgent
0x4beab020     2410     241    10000   0.00%  0.00%   0.00%   0         nvAgent
0x4be93020     3050     305    10000   0.00%  0.00%   0.00%   0    l2ProcMwpAck
0x4bd6e020     4210     421    10000   0.00%  0.00%   0.00%   0          L2Agent
0x4bd55020       80       8    10000   0.00%  0.00%   0.00%   0            dsagt
0x4bd39020        0       0        0   0.00%  0.00%   0.00%   0     ifaDispatch
0x4bb4f020     8530     853    10000   0.00%  0.33%   0.15%   0         ifagt_1
0x4baa8020      440      44    10000   0.00%  0.00%   0.00%   0         aclAgent
0x4ba74020     1430     143    10000   0.00%  0.00%   0.00%   0         sflPEAgt
```

```
0x4ba72020      560      56    10000   0.00%  0.00%   0.00%   0           count
0x4c679020     7120     712    10000   0.00%  0.00%   0.00%   0           PETmr
```

Example: show process cpu pe *pe-id* all

```
Dell#show processes cpu pe 255 all

      CPU Statistics Of PE-Unit 1 On PEID 255
     =======================================

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID       Runtime(ms)   Invok    uSecs   5Sec   1Min    5Min TTY        Process
0x4ba48020         20       2    10000   0.00%  0.00%   0.00%  0          POEAgt
0x4bb1f020        720      72    10000   0.00%  0.00%   0.00%  0         diagagt
0x4bb09020          0       0        0   0.00%  0.00%   0.00%  0       debugagt
0x4baf5020         10       1    10000   0.00%  0.00%   0.00%  0      F10StkMgr
0x4badf020       1320     132    10000   0.00%  0.00%   0.00%  0          envmgr
0x4bac9020       1420     142    10000   0.00%  0.00%   0.00%  0           lcMgr
0x4ba2f020       1220     122    10000   0.00%  0.00%   0.00%  0             dla
0x4ba0c020        410      41    10000   0.00%  0.00%   0.00%  0      sysAdmTsk
0x4b9f7020       4270     427    10000   0.00%  0.00%   0.00%  0         timerMgr
0x4b9e0020        260      26    10000   0.00%  0.00%   0.00%  0               PM
0x4b9c8020       9750     975    10000   0.00%  0.00%   0.00%  0               KP
0x4b9b2020          0       0        0   0.00%  0.00%   0.00%  0           evagt
0x4b995020        250      25    10000   0.00%  0.00%   0.00%  0             ipc
0x4b981020        120      12    10000   0.00%  0.00%   0.00%  0      sysReaper
0x4b927020         30       3    10000   0.00%  0.00%   0.00%  0             tme
0x4b912020          0       0        0   0.00%  0.00%   0.00%  0    ttraceIpFlow
0x4b8fc020          0       0        0   0.00%  0.00%   0.00%  0         isrTask
0x4af6f020          0       0        0   0.00%  0.00%   0.00%  0            tDDB
0x4af6e020         30       3    10000   0.00%  0.00%   0.00%  0              GC
0x4af6a020         20       2    10000   0.00%  0.00%   0.00%  0 linkscan_user_t
0x4af4e020          0       0        0   0.00%  0.00%   0.00%  0 bshell_reaper_t
0x4ab97020          0       0        0   0.00%  0.00%   0.00%  0         tSysLog
0x4ab87020        580      58    10000   0.00%  0.00%   0.00%  0      tTimerTask
0x4ab86020      18560    1856    10000   0.00%  0.00%   0.00%  0         tExcTask
0x4ab57020         20       2    10000   0.00%  0.00%   0.00%  0         tLogTask
0x4ab36020       9040     904    10000   0.00%  0.00%   0.00%  0          tUsrRoot
0x4068f020        100      10    10000   0.00%  0.00%   0.00%  0             main
0x4bea8020          0       0        0   0.00%  0.00%   0.00%  0     poePortScan
0x4c60c020       1060     106    10000   0.00%  0.00%   0.00%  0      V6RadAgent
0x4c5f3020        200      20    10000   0.00%  0.00%   0.00%  0         brAgent
0x4c5dd020          0       0        0   0.00%  0.00%   0.00%  0 nvProcessMwpAck
0x4c5c7020         40       4    10000   0.00%  0.00%   0.00%  0         IpAgent
0x4beab020       2890     289    10000   0.00%  0.00%   0.00%  0         nvAgent
0x4be93020       3700     370    10000   0.00%  0.00%   0.00%  0    l2ProcMwpAck
0x4bd6e020       5150     515    10000   0.00%  0.00%   0.00%  0         L2Agent
0x4bd55020         80       8    10000   0.00%  0.00%   0.00%  0           dsagt
0x4bd39020          0       0        0   0.00%  0.00%   0.00%  0     ifaDispatch
0x4bb4f020      10440    1044    10000   0.00%  0.17%   0.20%  0         ifagt_1
0x4baa8020        450      45    10000   0.00%  0.00%   0.00%  0        aclAgent
0x4ba74020       1740     174    10000   0.00%  0.00%   0.00%  0        sflPEAgt
0x4ba72020        680      68    10000   0.00%  0.00%   0.00%  0           count
0x4c679020       8620     862    10000   0.00%  0.00%   0.00%  0
```

Example: show processes cpu summary

```
Dell#show processes cpu summary

 CPU utilization    5Sec    1Min    5Min
 ----------------- ------- ------- --------
 CP                  43%     42%     40%
 RP                   0%      0%      0%
```

show processes ipc

Display the IPC messaging used internally between Dell Networking OS processes.

C9000 Series

Syntax

```
show processes ipc [recv-stats | send-stats] [cp | rp | lp | pe {slot-id | all}]
```

Parameters

recv-stats Enter the keyword `recv-stats` to display information on IPC receiver-side messages.

send-stats	Enter the keyword `send-stats` to display information on IPC sender-side messages.
cp	Enter the keyword `cp` to view IPC message statistics on the Control Processor CPU.
rp	Enter the keyword `rp` to view IPC message statistics on the Route Processor CPU.
lp *slot-id*	Enter the slot ID of the line card for which you want to view IPC message statistics. The range of switch slot IDs is from 0 to 11. Enter `linecard all` to view IPC statistics for all line cards.
pe *pe-id*	Enter the keyword `pe` to view IPC message statistics on the port extender (PE) .The PE ID range is from 0 to 255. **NOTE: The pe option is only visible when the extended bridge feature is enabled.**

Defaults

Display IPC message statistics on all switch CPUs: Control Processor, Route Processor, and line cards.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information

Important Points:

- Use `show processes ipc` commands only when you are working directly with Dell Technical Support to troubleshoot a problem.

Example: show processes ipc send-stats

```
Dell#show processes ipc send-stats rp
IPC Send Statistics on RP
Memory Used by Send DB on this processor: 1451880 bytes
SeqNo - Last sent guaranteed IPC pkt sequence no from this source to
destination
Success - No of successfull guaranteed IPC packets sent from source to
destination
1st-R -  No of first retry attempts
2nd-R -  No of second retry attempts
Fails -  No of guaranteed IPC pkts that could not be transmitted
RTT(ms) - Avg. Round Trip time for guaranteed IPC packets in millisecs
NonG-S -  No of non-guaranteed IPC pkts succesfully sent. This does not
include those sent by SWP
```

```
NonG-F -  No of non-guaranteed IPC pkt transmission failures
SWP-S -  No of non-guaranteed SWP IPC pkts succesfully sent
SWP-F -  No of non-guaranteed SWP IPC pkt transmission failures

Source->        Destination    SeqNo      Success   1st-R   2nd-R   Fails
RTT(ms)      NonG-S    NonG-F       SWP-S     SWP-FIPC: 1 ->              TME:
1    1561           3       0       0       0       2           0
0           0         0
IPC: 1 ->               IPC: 0   37025           0       0       0
0       0        1107          0           0         0
EVENTLOGAGENT: 1 ->    TME: 1   18888           0       0       0
0       0           1          0           0         0
EVENTLOGAGENT: 1 ->    TME: 1   18888           0       0       0
0       0           1          0           0         0
EVENTLOGAGENT: 1 ->    TME: 1   18888           0       0       0
0       0           1          0           0         0
EVENTLOGAGENT: 1 ->    TME: 1   18888           0       0       0
0       0           1          0           0         0
SYSADMTSK: 1 ->        TME: 1   26574           1       0       0
0       0           0          0           0         0
SYSADMTSK: 1 ->  SYSADMTSK: 0   21310           0       0       0
0       0        2251          0           0         0
SYSADMTSK: 1 ->    STATMGR: 0   21310           0       0       0
0       0        2251          0           0         0
ACL: 0 ->          UNKNOWN: 0   38997           1       0       0
0       0           0          0           0         0
ACL: 0 ->              TME: 4   24999           2       0       0
0       1           0          0           0         0
ACL: 0 ->              NMS:20   29588           1       1       1
1       0           0          0           0         0
RIP: 0 ->          ERRHDLR: 1   35003           0       0       0
0       0           1          0           0      ---------- More ----------
```

Example: show processes ipc recv-stats

```
Dell#show processes ipc recv-stats lp 2
IPC Receive Statistics on LP 2
Memory Used by Recv DB on this processor: 11172640 bytes
SeqNo - Last successfull Guaranteed IPC Pkt Seq No delivered from source to
destination
HiWtmk - Highest socket watermark reached for destination
M-SkSize - Max socket size of destination
NonG-Rcvd - No of non-guaranteed IPC pkts received
Pri-Dr - Priority drops done for non-guaranteed pkts due to socket almost-full
condition
SkFull-Dr - Any IPC packet dropped because of socket full condition

              Source->         Destination    SeqNo  HiWtmk(%)    M-SkSize
NonG-Rcvd  Pri-Dr SkFull-Dr
             TME: 0 ->              TME: 5       0         0
129024           1       0          0
             TME: 5 ->            LCMGR: 2       0         0
129024           1       0          0
             IPC: 0 ->              IPC: 5       0         0
129024        1084       0          0
             IPC: 5 ->              TME: 5   58307         0
129024           0       0          0
             CLI: 0 ->        SYSADMTSK: 5       0         0
129024          11       0          0
           CHMGR: 0 ->            LCMGR: 2   53689         0
129024           4       0          0
           LCMGR: 2 ->              TME: 5    3906         0
129024           1       0          0
           LCMGR: 2 ->    EVENTLOGAGENT: 5       0         0
129024           1       0          0
   EVENTLOGAGENT: 5 ->              TME: 5       0         0
129024           1       0          0
         DIAGMGR: 0 ->          DIAGAGT: 5       0         0
129024           1       0          0
         DIAGAGT: 5 ->              TME: 5    7899         0
```

```
129024           0       0           0
         DIAGAGT: 5 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
          EVHDLR: 0 ->             LCMGR: 2       0         0
129024           1       0           0
          EVHDLR: 0 ->              IFAGT: 2       0         0
129024           1       0           0
        DNLDAGENT: 5 ->               TME: 5    4759         1
129024           0       0           0
        DNLDAGENT: 5 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
        SYSADMTSK: 5 ->               TME: 5   40252         0
129024           0       0           0
        SYSADMTSK: 5 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
           PMMGR: 5 ->               TME: 5   62298         0
129024           0       0           0
           PMMGR: 5 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
            KPLR: 5 ->               TME: 5   36259         0
129024           0       0           0
            KPLR: 5 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
            KPLR: 5 ->             PMMGR: 5     604         0
129024           0       0           0
         TIMERMGR: 5 ->               TME: 5   14202         0
129024           0       0           0
        DEBUGAGNT: 5 ->               TME: 5      32         1
129024           0       0           0
        DEBUGAGNT: 5 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
        F10STKMGR: 5 ->               TME: 5   23990         0
129024           0       0           0
        F10STKMGR: 5 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
           ENVMGR: 5 ->               TME: 5   22188         1
129024           0       0           0
             ACL: 0 ->         ACL_AGENT: 2   24998         0
184320           8       0           0
        ACL_AGENT: 0 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
        ACL_AGENT: 2 ->               TME: 5   18120         0
129024           0       0           0
        ACL_AGENT: 2 ->             DSAGT: 2   35450         0
129024           0       0           0
        ACL_AGENT: 2 ->           FRRPAGT: 2   36661         0
163840           0       0           0
           IFAGT: 2 ->               TME: 5   17874         0
129024           0       0           0
           IFAGT: 2 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
             RTM: 0 ->            FIBAGT: 2       0         1
131072           5       0           0
             RTM: 0 ->              FIB6: 2       0         0
131072           3       0           0
          FIBAGT: 2 ->               TME: 5   15595         0
129024           0       0           0
          FIBAGT: 2 ->    EVENTLOGAGENT: 5       0         0
129024           1       0           0
          FIBAGT: 2 ->           TNLAGT: 2    3950         0
129024           0       0           0
         DIFFSERV: 0 ->         ACL_AGENT: 2   11562         2
184320           0       0           0
         DIFFSERV: 0 ->             DSAGT: 2       0         0
129024          10       0           0
           ARPMGR: 0 ->            FIBAGT: 2       0         0
129024           1       0           0
           MACMGR: 0 ->          MACAGENT: 2       0         0
129024           7       0           0
```

```
            DSAGT: 2 ->               TME: 5   35450          0
129024            0        0          0
            DSAGT: 2 ->    EVENTLOGAGENT: 5        0          0
129024            1        0          0
---------- More ----------
```

show processes ipc flow-control

Display Single Window Protocol Queue (SWPQ) statistics.

C9000 Series

Syntax `show processes ipc flow-control [cp | lp | pe | rp {slot-id | all}]`

Parameters

cp	Enter the keyword `cp` to view SWPQ statistics for the Control Processor CPU.
lp*slot-id*	Enter the slot ID of the line card for which you want to view IPC message statistics. The range of switch slot IDs is from 0 to 11. Enter `linecard all` to view IPC statistics for all line cards.
pe *pe-id*	Enter the keyword `pe` to view IPC message statistics on the port extender (PE) .The PE ID range is from 0 to 255. **NOTE: The pe option is only visible when the feature extended bridge is enabled.**
rp	Enter the keyword `rp` to view SWPQ statistics for the Route Processor CPU.

Defaults Display SWPQ statistics on all switch CPUs (Control Processor, Route Processor, and line cards).

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9 (0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information

Field	Description
Source QID /Tx Process	Source Service Identifier
Destination QID/Rx Process	Destination Service Identifier
Cur Len	Current number of messages enqueued
High Mark	Highest number of packets in the queue at any time
Timeout	Timeout count
Retries	Number of retransmissions
Msg Sent	Number of messages sent
Ack Rcvd	Number of messages acknowledged
Available Retra	Number of retries left
Max Retra	Number of retries allowed

Important Points:

- The SWP provides flow control-based reliable communication between the sending and receiving software tasks.
- A sending task enqueues messages into the SWP queue3 for a receiving task and waits for an acknowledgement.
- If no response is received within a defined period of time, the SWP timeout mechanism resubmits the message at the head of the FIFO queue.
- After retrying a defined number of times, the `SWP-2-NOMORETIMEOUT` timeout message is generated.
- A retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

Example

```
Dell#show processes ipc flow-control cp

 Q Statistics on CP Processor
    TxProcess     RxProcess       Cur       High   Time   Retr       Msg
Ack  Aval   Max
                                  Len       Mark   Out    ies        Sent
Rcvd Retra Retra
        DHCP0          ACL0         0          1      1      1
1         1    25    25
        DHCP0         IPMGR0        0          0      0      0
0         0    25    25
        DHCP0         IPMGR1        0          0      0      0
0         0    25    25
        DHCP0         IFMGR0        0          0      0      0
0         0    25    25
       IPMGR0          NDPM0        0          0      0      0
0         0    60    60
       IFMGR0          FEFD0        0         10      0      0
12        12    60    60
       IFMGR0          SNMP0        0          1      0      0
1         1    60    60
       IFMGR0       SFL_CP0         0         20      0      0
26        26    60    60
       IFMGR0     PORTMIRR0         0          8      0      0
9         9    60    60
       IFMGR0 EVENTTERMLOG0         0          1      0      0
1         1    60    60
       IFMGR0     IPSECMGR0         0          8      0      0
11        11    60    60
```

```
       IFMGR0          DHCP0          0           8      0      0
11        11    60    60
       IFMGR0         IPMGR0          0          29      0      0
36        36    60    60
       IFMGR0         IFAGT3          0           1      0      0
2         2     60    60
       IFAGT3         IFMGR0          0           1      0      0
1         1     60    60
       IFMGR0         OFMGR0          0          16      1      1
21        21    60    60
       IFMGR0          ACL0           0           8      0      0
14        14    60    60
       IFMGR0         VRRP0           0          10      0      0
17        17    60    60
       IFMGR0          PIM0           0           1      0      0
1         1     5     5
       IFMGR0        MACMGR0          0           0      0      0
0         0     60    60
       IFMGR0          L2PM0          0          29      0      0
40        40    60    60
       IFMGR0     DIFFSERV0           0          51      0      0
67        67    60    60
       IFMGR0          RTM0           0           9      0      0
11        11    60    60
       IFMGR0         LLDP0           0          12      0      0
12        12    60    60
       IFMGR0         MRTM0           0          10      0      0
10        10    60    60
       IFMGR0         IPMGR1          0          33      0      0
33        33    60    60
       IFMGR0         LACP0           0          23      0      0
23        23    60    60
    PORTMIRR0     ACL_AGENT2          0           0      0      0
0         0     50    50
       IFMGR0          IGMP0          0           0      0      0
0         0     50    50
       IFMGR0         IFAGT2          0           1      0      0
1         1     60    60
```

Example: show processes ipc flow-control pe

```
Dell#show processes ipc  flow-control pe 255 stack-unit 1

Q Statistics on PE unit 1 of PEID 255
    TxProcess     RxProcess       Cur       High   Time   Retr       Msg
Ack  Aval   Max
                                  Len       Mark   Out    ies        Sent
Rcvd Retra Retra
       BRAGT1         BRMGR0          0          2      0      0
2         2     25    25
     L2AGENT1        MACMGR0          0          0      0      0
0         0     90    90
       IFAGT1         IFMGR0          0          1      0      0
5         5     60    60
       IFAGT1         IFMGR0          0          50     0      0      74350
74350     60    60
      SFL_LP1        SFL_CP0          0          4      0      0
52        52     25    25
```

show processes memory

View information about memory usage for processes running in the system.

C9000 Series

Syntax

```
show processes memory [cp | lp {slot-id | all |summary} | pe {pe-id stack-unit unit-number | all | summary} | rp]
```

Parameters

cp	Enter the keyword `cp` to view memory usage for the Control Processor.
rp	Enter the keyword `rp` to view memory usage for the Route Processor.
lp *slot-id*	Enter the slot ID of the line card for which you want to view CPU memory usage. The range of switch slot IDs is from 0 to 2. Enter `linecard all` to display memory usage on all line card CPUs. Enter `linecard summary` to display a summary of memory usage on all line card CPUs.
pe *pe-id*	Enter the keyword `pe` and the port extender (PE) ID.*pe-id*. Range is from 0 to 255. **NOTE: The pe option is only visible when the feature extended bridge is enabled.**
stack-unit *unit-number*	Enter the keyword `stack-unit` and the stack *unit-number*. Range is from 0 to 7.

Command Modes

- EXEC
- EXEC Privilege

Defaults

Display detailed information on memory usage on all switch CPUs (Control Processor, Route Processor, Port Extender, and Line Cards).

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9 (0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.2	Introduced on the E-Series ExaScale E600i.
8.1.1.0	Introduced on the E-Series ExaScale E1200i.
7.5.1.0	Introduced on the C-Series.

Usage Information

show processes memory output Field	Description
Total:	Total system memory available
MaxUsed:	Total maximum memory used ever (history indicated with a time stamp)
CurrentUsed:	Total memory currently in use
CurrentFree:	Total system memory available
SharedUsed:	Total used shared memory
SharedFree:	Total free shared memory
PID	Process ID
Process	Process Name
ResSize	Actual resident size of the process in memory
Size	Process test, stack, and data size
Allocs	Total dynamic memory allocated
Frees	Total dynamic memory freed
Max	Maximum dynamic memory allocated
Current	Current dynamic memory in use

The output for `show process memory` displays the memory usage statistics running on the CP part (sysd) of the system. The sysd is an aggregate task that handles all the tasks running on the Control Processor.

The total counter size in `show memory` and `show processes memory` differs based on which OS processes are counted.

- In the `show memory` output, the memory size is equal to the size of the application processes.
- In the `show processes memory` output, the memory size is equal to the size of the application processes plus the size of the system processes.

In a dual homing setup, you can use this command only from the primary VLT peer.

Example: show processes memory

```
Dell#show processes memory
Total      :  3203928064, MaxUsed    :   804720640 [01/27/2014 06:16:44]
CurrentUsed:   804720640, CurrentFree:  2399207424
SharedUsed :     9776664, SharedFree :    16437760

 PID   Process         ResSize       Size    Allocs    Frees     Max
Current
 597 clish             3891200     106496         0        0         0         0
 631 login             4816896     217088         0        0         0         0
 464 ipSecMgr          4587520     274432    367528        0    367528    367528
 443 ssMgr             4059136     286720         0        0         0         0
 434 ipm               5287936    1208320    330360        0    330360    330360
 419 sysd             45555712   30474240   6584722   329480   6288190   6255242
 425 sysdlp           17965056   16535552         0        0         0         0
 427 sysmon             704512      24576         0        0         0         0
 421 sysmon             704512      24576         0        0         0         0
 398 flashmntr          843776      36864         0        0         0         0
 327 inetd              999424      45056         0        0         0         0
 244 sh                 860160    2301952         0        0         0         0
  74 sh                 737280    2301952         0        0         0         0
  30 mount_mfs        11755520    2310144         0        0         0         0
  25 mount_mfs       167346176    2310144         0        0         0         0
  22 mount_mfs         5226496    2310144         0        0         0         0
```

```
  19 mount_mfs        58314752     2310144        0        0        0          0
  12 mount_mfs          520192     2310144        0        0        0          0
   2 sh                 626688     2301952        0        0        0          0
   1 init               233472     2297856        0        0        0          0
   0 [system]         97353728           0        0        0        0          0
 506 sh                     0           0        0        0        0          0
ipc         34060          192       34060      33868
irc         943436         0         943436     943436
RpmAvailMgr 9376           32        9344       9344
ev          133188         0         133188     133188
evterm      26752          0         26752      26752
evhdlr      2528           8064      2528       0
dlm         7556256        7366960   1239104    189296
dla         416            0         416        416
tsm         15136          0         15136      15136
fmg         766560         0         766560     766560
fileProc    416            0         416        416
sysAdmTsk   42028          0         42028      42028
```

Example: show processes memory cp

```
Dell#show processes memory
Total      :  3203928064, MaxUsed    :   804720640 [01/27/2014 06:16:44]
CurrentUsed:   804720640, CurrentFree:  2399207424
SharedUsed :     9776664, SharedFree :    16437760

 PID   Process        ResSize      Size     Allocs     Frees     Max    Current
 597 clish            3891200     106496          0         0         0          0
 631 login            4816896     217088          0         0         0          0
 464 ipSecMgr         4587520     274432     367528         0    367528     367528
 443 ssMgr            4059136     286720          0         0         0          0
 434 ipm              5287936    1208320     330360         0    330360     330360
 419 sysd            45555712   30474240    6584722    329480   6288190    6255242
 425 sysdlp          17965056   16535552          0         0         0          0
 427 sysmon            704512      24576          0         0         0          0
 421 sysmon            704512      24576          0         0         0          0
 398 flashmntr         843776      36864          0         0         0          0
 327 inetd             999424      45056          0         0         0          0
 244 sh                860160    2301952          0         0         0          0
  74 sh                737280    2301952          0         0         0          0
  30 mount_mfs       11755520    2310144          0         0         0          0
  25 mount_mfs      167346176    2310144          0         0         0          0
  22 mount_mfs        5226496    2310144          0         0         0          0
  19 mount_mfs       58314752    2310144          0         0         0          0
  12 mount_mfs         520192    2310144          0         0         0          0
   2 sh                626688    2301952          0         0         0          0
   1 init              233472    2297856          0         0         0          0
   0 [system]        97353728          0          0         0         0          0
 506 sh                    0          0          0         0         0          0
ipc         34060          192       34060      33868
irc         943436         0         943436     943436
RpmAvailMgr 9376           32        9344       9344
ev          133188         0         133188     133188
evterm      26752          0         26752      26752
evhdlr      2528           8064      2528       0
dlm         7556256        7366960   1239104    189296
dla         416            0         416        416
tsm         15136          0         15136      15136
fmg         766560         0         766560     766560
fileProc    416            0         416        416
sysAdmTsk   42028          0         42028      42028
```

Example: show processes memory lp all

```
Dell#show processes memory lp summary

 Memory utilization   Total          MaxUsed       CurrentUsed   CurrentFree
 ------------------ -------------- -------------- -------------
--------------------
 LP2                  3203928064    384765952       8456566     3195471498
```

Example: show processes memory lp all

```
Dell#show processes memory lp all

     Memory Statistics Of Linecard Processor On Slot 2 (bytes)
     ==========================================================
Total:  3203928064, MaxUsed:   386670592, CurrentUsed:  386670592, CurrentFree:
2817257472
    TaskName  TotalAllocated       TotalFreed       MaxHeld    CurrentHolding
f10appioserv          163840                                         147456
      sysdlp        16543744                                       31641600
      sysmon           24576                                         704512
   flashmntr           36864                                         839680
       inetd           45056                                         995328
          sh         2301952                                         802816
          sh         2297856                                         708608
   mount_mfs         2310144                                       13471744
   mount_mfs         2310144                                       52310016
   mount_mfs         2310144                                        5226496
   mount_mfs         2310144                                       61145088
   mount_mfs         2310144                                         503808
          sh         2301952                                         626688
        init         2297856                                         233472
    [system]               0                                       88915968
         tme          433054              0        433054          433054
         ipc           33036              0         33036           33036
    timerMgr           66072              0         66072           66072
   sysAdmTsk           33036              0         33036           33036
       count           33036              0         33036           33036
       tFib4         2016720              0       2016720         2016720
    aclAgent         1490790              0       1490790         1490790
     ifagt_1          202348              0        202348          202348
       dsagt         1325606              0       1325606         1325606
    MacAgent          301474              0        301474          301474
        fib6         1654292              0       1654292         1654292
       ofagt          367522              0        367522          367522
      tnlagt          165180              0        165180          165180
     frrpagt          334400              0        334400          334400
```

Example: show processes memory rp

```
Dell#show processes memory rp

Total      :  3203928064, MaxUsed    :   376844288 [01/27/2014 06:16:47]
CurrentUsed:   376844288, CurrentFree:  2827083776
SharedUsed :     7993952, SharedFree :    18220472

 PID   Process            ResSize       Size       Allocs       Frees        Max
Current
 496 ofmgr                6000640      573440      896104           0      896104
896104
 392 ndpm                 5074944     1052672      301468           0      301468
301468
 160 vrrp                 5087232      434176      330360           0      330360
330360
 126 frrp                 4640768      282624      301362           0      301362
301362
 154 xstp                 8294400     4071424      466654           0      466654
466654
 118 pim                  8462336     1372160     3109852           0     3109852
3109852
 434 igmp                 5824512      655360      925008           0      925008
925008
 429 ipm1                 5255168      921600      396432           0      396432
396432
 170 mrtm                10838016     6123520     1127350           0     1127350
1127350
 294 l2mgr               18231296     1347584     1226308       32948     1226308
1193360
  98 l2pm                 4980736      294912     1520714     1120232      433430
400482
 389 arpm                 4644864      925696      301456           0      301456
301456
 367 lacp                 5390336      327680      598792           0      598792
598792
 349 tnlmgr               4554752      131072      466666           0      466666
466666
 329 otm                  4718592      258048      363396           0      363396
363396
```

```
 333 dsm                  7159808     2154496     1094262           0     1094262
1094262
 323 rtm                  8933376     1503232     3109744           0     3109744
3109744
 315 rip                  4362240      311296      198216           0      198216
198216
 309 acl                  6483968     1286144     1259692           0     1259692
1259692
 302 sysd                15392768     3305472      965786           0      965786
965786
 263 sysmon                704512       24576           0           0
0          0
 296 flashmntr             839680       36864           0           0
0          0
 198 inetd                 995328       45056           0           0
0          0
 122 sh                    802816     2301952           0           0
0          0
  74 sh                    708608     2297856           0           0
0          0
  30 mount_mfs           13467648     2310144           0           0
0          0
  25 mount_mfs           56033280     2310144           0           0
0          0
```

Example show processes memory pe 4 stack-unit 0

```
Dell#show processes memory pe 4 stack-unit  0
Total:  1073741824, MaxUsed:   343912448, CurrentUsed:  343896064, CurrentFree:
729845760
    TaskName  TotalAllocated       TotalFreed       MaxHeld    CurrentHolding
f10appioserv          184320                0             0          151552
       clish           57344                0             0         4845568
       login          163840                0             0         5197824
f10appioserv          184320                0             0          151552
       PEMgr          421888                0             0         9150464
f10appioserv          184320                0             0          151552
         brm         3051520                0             0        10440704
f10appioserv          184320                0             0          151552
        ipm1         1687552                0             0         6569984
f10appioserv          184320                0             0          151552
      sysdlp        22097920                0             0        32276480
f10appioserv          184320                0             0          151552
        sysd        31105024                0             0        43044864
   flashmntr           24576                0             0          827392
       inetd           49152                0             0         1077248
          sh         2641920                0             0          872448
          sh         2641920                0             0          757760
   mount_mfs         2654208                0             0         7393280
   mount_mfs         2654208                0             0         5124096
   mount_mfs         2654208                0             0        58220544
   mount_mfs         2654208                0             0          479232
          sh         2641920                0             0          610304
        init         2641920                0             0          188416
    [system]               0                0             0         1679360
         tme          220048                0        220048          220048
         ipc           16652                0         16652           16652
    timerMgr           33304                0         33304           33304
   sysAdmTsk           33212                0         33212           33212
       count              88                0            88              88
    sflPEAgt          965642           877892        104314           87750
    aclAgent           24232                0         24232           24232
     ifagt_1        38284252         38279404         87668            4848
       dsagt           24254                0         24254           24254
     L2Agent          286530                0        286530          286530
     nvAgent            4566                0          4566            4566
     brAgent          106006            49692         56314           56314
     frrpagt           38052                0         38052           38052
```

Example show processes memory pe 4 all

```
Dell#show processes memory pe 4  all

     Memory Statistics Of PE-unit Processor 0 On PEID 4 (bytes)
     ============================================================
Total:  1073741824, MaxUsed:   343920640, CurrentUsed:  343920640, CurrentFree:
729821184
    TaskName  TotalAllocated       TotalFreed       MaxHeld    CurrentHolding
```

```
f10appioserv          184320              0              0          151552
       clish           57344              0              0         4845568
       login          163840              0              0         5197824
f10appioserv          184320              0              0          151552
       PEMgr          421888              0              0         9150464
f10appioserv          184320              0              0          151552
         brm         3051520              0              0        10440704
f10appioserv          184320              0              0          151552
        ipm1         1687552              0              0         6569984
f10appioserv          184320              0              0          151552
      sysdlp        22097920              0              0        32301056
f10appioserv          184320              0              0          151552
        sysd        31105024              0              0        43044864
   flashmntr           24576              0              0          827392
       inetd           49152              0              0         1077248
          sh         2641920              0              0          872448
          sh         2641920              0              0          757760
   mount_mfs         2654208              0              0         7393280
   mount_mfs         2654208              0              0         5124096
   mount_mfs         2654208              0              0        58220544
   mount_mfs         2654208              0              0          479232
          sh         2641920              0              0          610304
        init         2641920              0              0          188416
    [system]               0              0              0         1679360
         tme          220048              0         220048          220048
         ipc           16652              0          16652           16652
    timerMgr           33304              0          33304           33304
   sysAdmTsk           33212              0          33212           33212
       count              88              0             88              88
    sflPEAgt          965642         877892         104314           87750
    aclAgent           24232              0          24232           24232
     ifagt_1        38367072       38362224          87668            4848
       dsagt           24254              0          24254           24254
     L2Agent          286530              0         286530          286530
     nvAgent            4566              0           4566            4566
     brAgent          106006          49692          56314           56314
     frrpagt           38052              0          38052           38052
```

Example show processes memory pe 4 summary

```
Dell#show processes memory pe 4  summary

 Memory utilization  Total      MaxUsed    CurrentUsed  CurrentFree
 ------------------ ---------- ---------- ----------- -----------
 PE-UNIT0           1073741824   343896064  343846912    729894912
```

show reset-reason

Display the reason for the last system reboot.

Syntax

```
show reset-reason
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13(0.0)	Introduced on the S3048–ON, S3100 series, S4048–ON, S4048T–ON, S5000, S6000, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, C9010, MXL, M-IOA, and FN-IOM.

Usage Information

You can use the `show reset-reason` without the `stack-unit` option to view the reason for the last system reboot of the local system.

Example — Unknown reason

If the reason for the last system reboot is not available, the system displays the reason as N/A.

```
DellEMC# show reload-reason
Cause: N/A
Time: N/A
```

Example

```
DellEMC# show reset-reason
Last Reset Reason:
--------------------
Type                Cause                                   Time
-------------------------------------------------------------------------------
rpm 0 (CP)          Reboot by Software                      11/05/2017-08:05
rpm 0 (RP)          Reboot by Software                      11/05/2017-08:05
rpm 1 (CP)          Power on Reset                          N/A
rpm 1 (RP)          Power on Reset                          N/A
linecard 0          N/A                                     N/A
linecard 1          N/A                                     N/A
linecard 2          N/A                                     N/A
linecard 3          N/A                                     N/A
linecard 4          Warm Reset                              N/A
linecard 5          N/A                                     N/A
linecard 6          N/A                                     N/A
linecard 7          N/A                                     N/A
linecard 8          N/A                                     N/A
linecard 9          N/A                                     N/A
linecard 10         Power on Reset                          N/A
linecard 11         Power on Reset                          N/A
```

```
DellEMC#show reset-reason pe all

Last Reset Reason:
----------------------
Type                  Cause                                     Time
-------------------------------------------------------------------------------

PE ID: 10
==========
stack-unit 0        N/A                                       N/A
stack-unit 1        N/A                                       N/A
stack-unit 2        N/A                                       N/A
stack-unit 3        Reboot by Software                        11/02/2017-08:15
stack-unit 4        N/A                                       N/A
stack-unit 5        N/A                                       N/A
stack-unit 6        N/A                                       N/A
stack-unit 7        N/A                                       N/A

PE ID: 20
==========
stack-unit 0        N/A                                       N/A
stack-unit 1        Reboot by Software                        11/02/2017-04:10
stack-unit 2        N/A                                       N/A
stack-unit 3        N/A                                       N/A
stack-unit 4        N/A                                       N/A
stack-unit 5        N/A                                       N/A
stack-unit 6        N/A                                       N/A
stack-unit 7        N/A                                       N/A
```

show rpm

View the current status of the RPM.

C9000 Series

Syntax

```
show rpm [slot-id [brief] | all]
```

Parameters

slot-id	(OPTIONAL) Enter the RPM slot-ID zero (`0`) or `1`.
all	(OPTIONAL) Enter the keyword `all` to view a table with information on all present RPMs.
brief	(OPTIONAL) Enter the keyword `brief` to view an abbreviated list of RPM information.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

Field	Description
Status	Displays the RPM's status.
Next Boot	Displays whether the RPM is to be brought online at the next system reload.
Card Type	Displays the RPM catalog number.
Hardware Rev	Displays the hardware revision level.
Num Ports	Displays the number of active ports.
Up Time	Displays the number of hours and minutes since the RPM's last reboot.
Last Restart	States the reason for the last RPM reboot.
Dell Networking OS Version	Displays the operating software version.
Jumbo Capable	Displays a Yes or No indicating if the RPM is capable of sending and receiving Jumbo frames.

Field	Description
	This field does not indicate if the chassis is in Jumbo mode; for that determination, use the `show chassis brief` command.
CP Boot Flash	Displays the two possible Boot Flash versions for the control processor. The [Booted] keyword next to the version states which version was used at system boot.
RP Boot Flash	Displays the Boot Flash version for the Routing Processor. The [Booted] keyword next to the version states which version was used at system boot.
CP Mem Size	Displays the memory of the control processor.
RP Mem Size	Displays the memory of the Routing Processor.
Temperature	Displays the temperature of the RPM. Minor alarm status if the temperature is over 65°C.
Power Status	Lists the status of the power modules in the chassis.
Voltage	Displays the power rails for the line card.
Part Num	Displays the line card part number.
Vendor ID	Displays an internal code, which specifies the manufacturing vendor.
Date Code	Displays the line card's manufacturing date.
Country Code	Displays the country of origin. 01 = USA.

Example

```
Dell#show rpm 0

-- RPM card 0 --
Status        : active
Next Boot     : online
Card Type     : RPM - Route Processor Module (C9000-RPM-2.56T)
Hardware Rev  : 4.0
Num Ports     : 1
Up Time       : 21 min, 28 sec
Last Restart  : normal power-cycle
Dell Networking OS Version : 9.9(0.0)
Jumbo Capable : yes
CP Boot Flash : 3.3.1.16  [booted]
RP Boot Flash : 3.3.1.16  [booted]
Boot Selector : 3.3.0.1
RP Boot Selector : 3.3.0.1
CP Mem Size   : 2127536128 bytes
RP Mem Size   : 2127536128 bytes
Temperature   : 28C 54C
Power Status  : AC
Voltage       : ok
Serial Number : NA
Part Number   : 0CKKCP     Rev X00
Vendor Id     : NA
Date Code     : NA
Country Code  : NA
Piece Part ID : CN-0CKKCP-77931-466-0009
PPID Revision : X00
Service Tag   : 13NRG02
Expr Svc Code : 239 809 248 2
Auto reboot   : Disabled
```

```
Dell#show rpm 0 brief

-- RPM card 0 --
Status        : active
Next Boot     : online
Card Type     : RPM - Route Processor Module (C9000-RPM-2.56T)
Hardware Rev  : 4.0
```

```
Num Ports      : 1
Up Time        : 32 min, 25 sec
Last Restart   : normal power-cycle
Dell Networking OS Version : 9.9(0.0)
Jumbo Capable : yes
```

```
Dell#show rpm all

--  Route Processor Modules --
Slot  Status        NxtBoot     Version
-------------------------------------------------------
  0   active        online      9.9(0.0)
  1   booting
```

Related Commands

- show chassis – view information on all elements of the system.
- show linecard– view information on a line card.

show software ifm

Display interface management (IFM) data.

C9000 Series

Syntax

```
show software ifm {clients [summary] | ifagt number | ifcb interface | linecard slot-id | trace-flags}
```

Parameters

clients	Enter the keyword `clients` to display IFM client information.
summary	(OPTIONAL) Enter the keyword `summary` to display brief information about IFM clients.
ifagt *number*	Enter the keyword `ifagt` then the number of an interface agent to display software pipe and IPC statistics.
ifcb *interface*	Enter the keyword `ifcb` then one of the following interface IDs then the slot/port information to display interface control block information for that interface: • For a Port Channel interface, enter the keyword `port-channel` then a number: The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.
linecard *slot-id*	Enter the `linecard` *`slot-id`* parameters to specify the switch ports on a line card. The range of slot IDs is from 0 to 11.
trace-flags	Enter the keyword `trace-flags` to display IFM information for internal trace flags.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9 (0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
7.6.1.0	Introduced for the C-Series and S-Series.

Example

```
Dell# show software ifm clients summary
ClntType Inst svcMask subSvcMask tlvSvcMask tlvSubSvc swp
IPM      0 0x00000000 0x00000000 0x90ff71f3 0x021e0e81 31
RTM      0 0x00000000 0x00000000 0x800010ff 0x01930000 43
VRRP     0 0x00000000 0x00000000 0x803330f3 0x00400000 39
L2PM     0 0x00000000 0x00000000 0x87ff79ff 0x0e032200 45
ACL      0 0x00000000 0x00000000 0x867f50c3 0x000f0218 44
OSPF     0 0x00000dfa 0x00400098 0x00000000 0x00000000 0
PIM      0 0x000000f3 0x00030000 0x00000000 0x00000000 0
IGMP     0 0x000e027f 0x00000000 0x00000000 0x00000000 0
SNMP     0 0x00000000 0x00000000 0x800302c0 0x00000002 30
EVTTERM  0 0x00000000 0x00000000 0x800002c0 0x00000000 29
MRTM     0 0x00000000 0x00000200 0x81f7103f 0x00000000 38
DSM      0 0x00000000 0x00000000 0x80771003 0x00000000 32
LACP     0 0x00000000 0x00000000 0x8000383f 0x00000000 35
DHCP     0 0x00000000 0x00000000 0x800000c2 0x0000c000 37
V6RAD    0 0x00000433 0x00030000 0x00000000 0x00000000 0
Unidentified Client0 0x006e0002 0x00000000 0x00000000 0x00000000 0
Dell#
```

```
Dell#show software ifm linecard 0
linecard: 0
        cardType = 516                          numPorts = 144
        numCfgPorts = 0                         cardId = 0x7f0a0a0d
        cardState = 3                           prevHello = 0:0
        notifSeqNum = 1                         ifaNotifSeqNum = 0 0
        cardAlive = 0                           pStatusMask = 0xffffffff
        ppStatus[0] = 0x00000001                ppStatus[1] = 0x00000001
```

```
Dell# show software ifm linecard 0 | find cardstate ignore-case
        cardState = 3                           prevHello = 0:0
        notifSeqNum = 1                         ifaNotifSeqNum = 0 0
        cardAlive = 0                           pStatusMask = 0xffffffff
        ppStatus[0] = 0x00000001                ppStatus[1] = 0x00000001
```

```
Dell# show software ifm linecard 0 | save flash://sh_sf_ifm_linecard0
Start saving show command report .......
```

show system linecard

Display the status of a specified linecard.

Syntax `show system linecard slot-id fanout {configured | count}`

Parameters

slot-id	Enter the linecard slot-id. The slot-id range is from 0 to 11.

	count	Enter the keyword `count` to view the fanout ports configured or present on a linecard.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Example

```
Dell#sh system linecard 6 fanout configured
Configured fan out ports in linecard 6
Configured Present
0 0
4 4
8 8
12 12
16 16
20 20
```

```
Dell#sh system linecard 6 fanout count
Fan out ports in linecard 6
Configured = 6
Present = 6
```

show tech-support

Display a collection of data from other `show` commands, necessary for Dell Networking technical support to troubleshoot switch operation.

C9000 Series

Syntax

`show tech-support [linecard` *`slot-id`* `| page | pe` *`pe-id`* `stack-unit` *`unit-number`*`]`

From a **PE console**, use `show tech-support stack-unit` *`unit-number`* `page`

Parameters

linecard *slot-id*	Enter the slot ID of the line card for which you want to collect information for tech support. The range of slot IDs is from 0 to 11. Enter `linecard all` to collect troubleshooting information on all line cards.
page	(OPTIONAL) Enter the keyword `page` to view 24 lines of text at a time. Press the SPACE BAR to view the next 24 lines. Press the ENTER key to view the next line of text.
pe *pe-id*	(OPTIONAL) Enter the keyword `pe` and the port extender(PE) ID. The PE ID range is from 0 to 255.

NOTE: The pe option is only visible when the extended bridge feature is enabled.

stack-unit *unit-number*	Enter the keyword `stack-unit` and the unit number. The stack-unit range is from 0 to 7.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9 (0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced `save` to the file options.
7.6.1.0	Introduced on the S-Series.

Usage Information Without the `page or linecard` option, the command output is continuous. To interrupt the command output, use Ctrl-z.

The `save` option works with other filtering commands. This allows you to save specific information of a `show` command. The `save` entry must always be the last option. For example: `Dell#show tech-support |grep regular-expression |except regular-expression | find regular-expression | save flash://result`

This display output is an accumulation of the same information that is displayed when you execute one of the following `show` commands:

- `show clock`
- `show control-bridge status`
- `show environment`
- `show HA information`
- `show interfaces`
- `show inventory`
- `show lldp neighbors`
- `show processes cpu`
- `show processes cpu summary`
- `show processes memory`
- `show running-conf`
- `show system stack-ports`
- `show version`

Example

```
Dell#show tech-support linecard 0
---------------------------------- show version ----------------------------
Dell Real Time Operating System Software
Dell Operating System Version: 2.0
Dell Application Software Version: 1-0(0-4095)
Copyright (c) 1999-2015 by Dell Inc. All Rights Reserved.
```

```
Build Time: Thu Jun 25 18:00:00 2015
Build Path: /build/build01/SW/SRC
Dell Networking OS uptime is 59 minute(s)
System image file is "system://A"
System Type: C9010
Control Processor:Intel Rangeley with 2 Gbytes (2127536128 bytes) of memory, core(s) 2.
Route Processor:Intel Rangeley with 2 Gbytes (2127536128 bytes) of memory, core(s) 2.
16G bytes of boot flash memory.
2 Route Processor Module.
3 24-port TE/GE
3 24-port TE/GE
4 6-port TE/FG
2 4-port TE/GE
200 Ten GigabitEthernet/IEEE 802.3 interface(s)
12 Forty GigabitEthernet/IEEE 802.3 interface(s)
---------------------------------- show linecard 0 verbose ------------
-- Linecard 0 --
Status : online
Next Boot : online
Required Type : C9000LC2410T - 24-port TE/GE
Current Type : C9000LC2410T - 24-port TE/GE
Hardware Rev : 4.0
Num Ports : 24
Up Time : 57 min, 21 sec
Dell Networking OS Version : 1-0(0-4095)
Jumbo Capable : yes
POE Capable : Not supported
Max Required Power : 205
Boot Flash : 3.3.1.15
Boot Selector : 3.3.0.0g
Memory Size : 2127654912 bytes
Serial Number :
Part Number : 0KFHFG Rev X00
Vendor Id :
Date Code :
Country Code :
Piece Part ID : CN-0KFHFG-77931-4A5-0022
PPID Revision : X00
Service Tag : 15DSG02
Expr Svc Code : 250 227 533 0
Flash Boot : A: 1-0-0-4095 B: 1-0-0-4072 Booted from: A: 1-0-0-4095
Auto Reboot : enabled
Last Restart : powered-on
Burned In MAC : 34:17:eb:01:8c:00
No Of MACs : 3
---------------------------------- show environment linecard-voltage -----
-- Fan Status --
Unit Bay TrayStatus Fan0 Speed Fan1 Speed Fan2 Speed Fan3 Speed
-------------------------------------------------------------------------
0 0 up up 3587 up 3558 up 3591 up 3539
0 1 up up 3558 up 3476 up 3539 up 3614
0 2 up up 3817 up 3640 up 3552 up 3699
Speed in RPM
-- Power Supplies --
Unit Bay Status Type FanStatus FanSpeed(rpm) Power Usage (W)
-------------------------------------------------------------------------
0 0 up AC up 3072 292.5
0 1 up AC up 3088 233.2
0 2 up AC up 3072 249.5
0 3 up AC up 3072 253.2
Total power: 1028.5 W
-- Thermal Sensor Readings (deg C) --
Slot 0 1 2 3 4 5 6 7 8 9
-----------------------------------------------------------------
     75 67 68 60 78 73 65 58 73 61
------------------------- show process memory on Linecard 0 ----------------
Total: 2127654912, MaxUsed: 406441984, CurrentUsed: 406417408,
CurrentFree: 1721237504
TaskName TotalAllocated TotalFreed MaxHeld CurrentHolding
f10appioserv 163840 0 0 86016
sysdlp 35016704 0 0 57663488
sysmon 24576 0 0 380928
sh 2433024 0 0 454656
flashmntr 61440 0 0 577536
inetd 45056 0 0 618496
rngd 32768 0 0 376832
mount_mfs 2441216 0 0 71548928
```

```
sh 2433024 0 0 634880
init 2428928 0 0 229376
[system] 0 0 0 111058944
sh 0 0 0 0
sh 0 0 0 0
tme 433054 0 433054 433054
ipc 33036 0 33036 33036
timerMgr 66072 0 66072 66072
sysAdmTsk 33036 0 330
```

Example (PE Console)

```
Dell#show tech-support
----------------------------- show version -----------------------------
Dell Real Time Operating System Software
Dell Operating System Version:  2.0
Dell Application Software Version:  9.9(0.0)
Copyright (c) 1999-2015 by Dell Inc. All Rights Reserved.
Build Time: Tue Sep  8 03:51:15 2015
Build Path: /sites/eqx/work/swbuild01_1/patch02/E9-9-0/SW/SRC
Dell Networking OS uptime is 6 day(s), 21 hour(s), 14 minute(s)

System image file is "system://B"

System Type: C1048P
Control Processor: Broadcom 56340 (ver A0)
with 1 Gbytes (1073741824 bytes) of memory, core(s) 1.

16G bytes of boot flash memory.

  2 48-port GE
96 GigabitEthernet/IEEE 802.3 interface(s)

----------------------------------- show clock --------------------------
11:41:10.577 UTC Thu Sep 17 2015

---------------------------------- show HA information -------------

--  Stack-unit Status  --
-----------------------------------------------
Mgmt ID:                        0
Stack-unit ID:                  1
Stack-unit Redundancy Role:     Primary
Stack-unit State:               Active
Stack-unit SW Version:          9.9(0.0)
Link to Peer:                   Up

--  PEER Stack-unit Status  --
-----------------------------------------------
Stack-unit State:               Standby
Peer Stack-unit ID:             3
Stack-unit SW Version:          9.9(0.0)

--  Stack-unit Redundancy Configuration  --
-----------------------------------------------
Primary Stack-unit:             mgmt-id    0
Auto Data Sync:                 Full
Failover Type:                  Hot Failover
Auto reboot Stack-unit:         Enabled
Auto failover limit:            3 times in 60 minutes

--  Stack-unit Failover Record  --
-----------------------------------------------
Failover Count:                 0
Last failover timestamp:        None
Last failover Reason:           None
Last failover type:             None

--  Last Data Block Sync Record:  --
-----------------------------------------------
stack-unit Config:         succeeded  Sep 08 2015 13:07:32
Runtime Event Log:         succeeded  Sep 08 2015 13:07:32
    Running Config:         succeeded  Sep 08 2015 13:07:32

---------------------------------- show system stack-ports --------------
Topology: Daisy chain
Interface  Connection    Link Speed      Admin     Link
                           (Gb/s)        Status    Status
```

```
-------------------------------------------------------
  1/1         3/1           24             up        up
  1/2                       24             up        down
  3/1         1/1           24             up        up
  3/2                       24             up        down

---------------------------------- show interface ----------------------
TenGigabitEthernet 0/1 is up, line protocol is not present
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
Interface index is 1054730
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 1000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:00:00
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d20h19m


TenGigabitEthernet 0/2 is up, line protocol is not present
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
Interface index is 1054858
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 1000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:00:00
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d20h19m


TenGigabitEthernet 1/1 is up, line protocol is up
Port is part of Port-channel 257
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    No power
Interface index is 2103306
```

```
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 10000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 6d20h19m
Queueing strategy: fifo
Input Statistics:
     4062996 packets, 799504603 bytes
     0 64-byte pkts, 193370 over 64-byte pkts, 3869429 over 127-byte pkts
     2 over 255-byte pkts, 20 over 511-byte pkts, 175 over 1023-byte pkts
     193229 Multicasts, 0 Broadcasts, 3869767 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     3978357 packets, 4298183062 bytes, 0 underruns
     0 64-byte pkts, 110 over 64-byte pkts, 187904 over 127-byte pkts
     94 over 255-byte pkts, 17498 over 511-byte pkts, 3772751 over 1023-byte pkts
     187593 Multicasts, 0 Broadcasts, 3790764 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d20h19m


TenGigabitEthernet 1/2 is up, line protocol is down
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
Pluggable media not present
Interface index is 2103434
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 6d21h14m
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d21h13m

TenGigabitEthernet 3/1 is up, line protocol is up
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    No power
Interface index is 4200458
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 10000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 6d21h13m
Queueing strategy: fifo
Input Statistics:
     1342099159 packets, 1072976665217 bytes
     0 64-byte pkts, 50445671 over 64-byte pkts, 118407762 over 127-byte pkts
     236832324 over 255-byte pkts, 472286757 over 511-byte pkts,
```

```
     464126645 over 1023-byte pkts
     24422 Multicasts, 0 Broadcasts, 1342074737 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     1342667555 packets, 1073326413846 bytes, 0 underruns
     0 64-byte pkts, 50456645 over 64-byte pkts, 118609785 over 127-byte pkts
     236899846 over 255-byte pkts, 472421536 over 511-byte pkts,
     464279743 over 1023-byte pkts
     210075 Multicasts, 0 Broadcasts, 1342457480 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d21h13m

Port-channel 257 is up, line protocol is up
Created by Auto LAG
Hardware address is f8:b1:56:62:61:0a, Current address is f8:b1:56:62:61:0a
Interface index is 1258422784
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 10000 Mbit
Members in this channel:  Te 1/1(U)
ARP type: ARPA, ARP Timeout 04:00:00
Queueing strategy: fifo
Input Statistics:
     4062996 packets, 799504603 bytes
     0 64-byte pkts, 193370 over 64-byte pkts, 3869429 over 127-byte pkts
     2 over 255-byte pkts, 20 over 511-byte pkts, 175 over 1023-byte pkts
     193229 Multicasts, 0 Broadcasts, 3869767 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     3978357 packets, 4298183062 bytes, 0 underruns
     0 64-byte pkts, 110 over 64-byte pkts, 187904 over 127-byte pkts
     94 over 255-byte pkts, 17498 over 511-byte pkts, 3772751 over 1023-byte pkts
     187593 Multicasts, 0 Broadcasts, 3790764 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d21h13m


Vlan 1 is down, line protocol is down
Address is f8:b1:56:62:61:0a, Current address is f8:b1:56:62:61:0a
Interface index is 1275068928
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 6d21h13m
Queueing strategy: fifo
Time since last interface status change: 6d21h13m

--------------------------- show process memory ------------------

     Memory Statistics Of stack-unit 1 (bytes)
     ============================================================
Total: 1073741824, MaxUsed: 351678464, CurrentUsed: 351629312, CurrentFree: 722112512
    TaskName      TotalAllocated     TotalFreed     MaxHeld    CurrentHolding
    f10appioserv          180224              0           0            147456
           clish           57344              0           0           4759552
           login          163840              0           0           5423104
         telnetd           77824              0           0           1032192
    f10appioserv          184320              0           0            151552
           PEMgr          442368              0           0           9748480
    f10appioserv          180224              0           0            147456
             brm         3084288              0           0           9973760
    f10appioserv          180224              0           0            147456
            ipm1         5087232              0           0           4988928
```

```
    f10appioserv          184320            0             0          151552
          sysdlp        23752704            0             0        36388864
    f10appioserv          180224            0             0          147456
           sysd         31113216            0             0        43839488
      flashmntr            24576            0             0          860160
          inetd            49152            0             0         1060864
             sh          2646016            0             0          835584
             sh          2646016            0             0          733184
      mount_mfs          2658304            0             0         7741440
      mount_mfs          2658304            0             0         5144576
      mount_mfs          2658304            0             0        59711488
      mount_mfs          2658304            0             0          450560
             sh          2646016            0             0          593920
           init          2646016            0             0          184320
       [system]                0            0             0         1802240
            tme           220048            0        220048          220048
            ipc            16652            0         16652           16652
       timerMgr            33304            0         33304           33304
      sysAdmTsk            33212            0         33212           33212
          count               88            0            88              88
       sflPEAgt          2704862      2583984        137442          120878
       aclAgent            24232            0         24232           24232
        ifagt_1       3272338996   3272334148        104232            4848
          dsagt            24254            0         24254           24254
       L2Agent          1247242       612868        650938          634374
       nvAgent             4566            0          4566            4566
       brAgent           155698        82820         72878           72878

     Memory Statistics Of stack-unit 3 (bytes)
     =========================================================
Total: 1073741824, MaxUsed: 340434944, CurrentUsed: 340385792, CurrentFree: 733356032
    TaskName      TotalAllocated       TotalFreed       MaxHeld    CurrentHolding
         login          163840             0             0         5050368
  f10appioserv          184320             0             0          151552
         PEMgr          442368             0             0         8314880
  f10appioserv          180224             0             0          147456
           brm         3084288             0             0         9388032
  f10appioserv          180224             0             0          147456
          ipm1         5087232             0             0         4894720
  f10appioserv          184320             0             0          151552
        sysdlp        23752704             0             0        36401152
  f10appioserv          180224             0             0          147456
          sysd         31113216             0             0        43417600
     flashmntr            24576             0             0          839680
         inetd            49152             0             0         1060864
            sh          2646016             0             0          835584
            sh          2646016             0             0          733184
     mount_mfs          2658304             0             0         7741440
     mount_mfs          2658304             0             0         5144576
     mount_mfs          2658304             0             0        59547648
     mount_mfs          2658304             0             0          450560
            sh          2646016             0             0          593920
          init          2646016             0             0          184320
      [system]                0             0             0         1687552
           tme           220048             0        220048          220048
           ipc            16652             0         16652           16652
      timerMgr            33304             0         33304           33304
     sysAdmTsk            33212             0         33212           33212
         count               88             0            88              88
      sflPEAgt          2605478       2484600        137442          120878
      aclAgent           305820        281588        156744           24232
       ifagt_1       3272305868    3272301020        104232            4848
         dsagt            24254             0         24254           24254
       L2Agent          1247242       612868        650938          634374
       brAgent           155698        82820         72878           72878
       nvAgent             4566            0          4566            4566

---------------------------------- show process cpu -----------------------

      CPU Statistics Of Unit 1
     ======================================

CPU utilization for five seconds: 1%/0%; one minute: 0%; five minutes: 0%
PID        Runtime(ms) Invoked  uSecs  5Sec   1Min  5Min  TTY      Process
0x4bc86020  3982860  398286   10000  1.00%  0.67%  0.48%  0         ifagt_1
0x4bc50020   127380   12738   10000  0.00%  0.00%  0.00%  0         diagagt
0x4bc3a020        0       0       0  0.00%  0.00%  0.00%  0        debugagt
```

```
0x4bc25020       30       3   10000  0.00%  0.00%  0.00%  0       F10StkMgr
0x4bc10020   242100   24210   10000  0.00%  0.00%  0.00%  0          envmgr
0x4bb76020   222230   22223   10000  0.00%  0.00%  0.00%  0           lcMgr
0x4bb60020    15370    1537   10000  0.00%  0.00%  0.00%  0             dla
0x4bb3d020    71010    7101   10000  0.00%  0.00%  0.00%  0       sysAdmTsk
0x4bb27020   759200   75920   10000  0.00%  0.00%  0.00%  0        timerMgr
0x4bb10020    53930    5393   10000  0.00%  0.00%  0.00%  0              PM
0x4baf8020  1928170  192817   10000  0.00%  0.08%  0.00%  0              KP
0x4bae2020        0        0       0  0.00%  0.00%  0.00%  0          evagt
0x4bac5020    40140    4014   10000  0.00%  0.00%  0.00%  0             ipc
0x4bab1020    13800    1380   10000  0.00%  0.00%  0.00%  0       sysReaper
0x4ba56020       40       4   10000  0.00%  0.00%  0.00%  0             tme
0x4ba41020        0        0       0  0.00%  0.00%  0.00%  0    ttraceIpFlow
0x4ba2a020        0        0       0  0.00%  0.00%  0.00%  0         isrTask
0x4b1ba020        0        0       0  0.00%  0.00%  0.00%  0           tDDB
0x4b1a6020     5390      539   10000  0.00%  0.00%  0.00%  0              GC
0x4b174020       50        5   10000  0.00%  0.00%  0.00%  0 linkscan_user_t
0x4af77020        0        0       0  0.00%  0.00%  0.00%  0 bshell_reaper_t
0x4abcc020        0        0       0  0.00%  0.00%  0.00%  0         tSysLog
0x4ab9f020   106760   10676   10000  0.00%  0.00%  0.00%  0      tTimerTask
0x4ab6f020  3480010  348001   10000  0.00%  0.00%  0.05%  0        tExcTask
0x4ab5f020       20        2   10000  0.00%  0.00%  0.00%  0        tLogTask
0x4ab3e020    68110    6811   10000  0.00%  0.00%  0.00%  0        tUsrRoot
0x40697020      590       59   10000  0.00%  0.00%  0.00%  0            main
0x4c593020        0        0       0  0.00%  0.00%  0.00%  0 nvProcessMwpAck
0x4c17a020      370       37   10000  0.00%  0.00%  0.00%  0         brAgent
0x4be61020   494050   49405   10000  0.00%  0.00%  0.02%  0         nvAgent
0x4be4a020   569630   56963   10000  0.00%  0.00%  0.00%  0    l2ProcMwpAck
0x4bd28020   887440   88744   10000  0.00%  0.00%  0.00%  0         L2Agent
0x4bd0f020      230       23   10000  0.00%  0.00%  0.00%  0           dsagt
0x4bcf4020        0        0       0  0.00%  0.00%  0.00%  0     ifaDispatch
0x4bb7b020       30        3   10000  0.00%  0.00%  0.00%  0          POEAgt
0x4bb86020     7240      724   10000  0.00%  0.00%  0.00%  0        aclAgent
0x4bbbe020   267310   26731   10000  0.00%  0.00%  0.00%  0        sflPEAgt
0x4bbbb020   129340   12934   10000  0.00%  0.00%  0.00%  0           count
0x4bba7020        0        0       0  0.00%  0.00%  0.00%  0     poePortScan
0x4c77a020  1612410  161241   10000  0.00%  0.00%  0.00%  0           PETmr

      CPU Statistics Of Unit 3
     ========================================

CPU utilization for five seconds: 0%/0%; one minute: 0%; five minutes: 0%
PID        Runtime(ms) Invoked  uSecs  5Sec   1Min   5Min TTY      Process
0x4bb7c020       20         2  10000  0.00%  0.00%  0.00% 0         POEAgt
0x4bb7a020   128330     12833  10000  0.00%  0.00%  0.00% 0        diagagt
0x4bc3a020        0         0      0  0.00%  0.00%  0.00% 0       debugagt
0x4bc26020       10         1  10000  0.00%  0.00%  0.00% 0      F10StkMgr
0x4bc10020   252250     25225  10000  0.00%  0.00%  0.00% 0         envmgr
0x4bb62020   244950     24495  10000  0.00%  0.00%  0.00% 0          lcMgr
0x4bb61020    15800      1580  10000  0.00%  0.00%  0.00% 0            dla
0x4bb3e020    81220      8122  10000  0.00%  0.00%  0.00% 0      sysAdmTsk
0x4bb27020   762400     76240  10000  0.00%  0.00%  0.00% 0       timerMgr
0x4bb10020    52680      5268  10000  0.00%  0.00%  0.00% 0             PM
0x4baf8020  1900590    190059  10000  0.00%  0.00%  0.00% 0             KP
0x4bae2020        0         0      0  0.00%  0.00%  0.00% 0          evagt
0x4bac5020    60440      6044  10000  0.00%  0.00%  0.00% 0            ipc
0x4bab1020    13660      1366  10000  0.00%  0.00%  0.00% 0      sysReaper
0x4ba56020       40         4  10000  0.00%  0.00%  0.00% 0            tme
0x4ba41020        0         0      0  0.00%  0.00%  0.00% 0   ttraceIpFlow
0x4ba2a020        0         0      0  0.00%  0.00%  0.00% 0        isrTask
0x4b1ba020       10         1  10000  0.00%  0.00%  0.00% 0           tDDB
0x4b1a6020     5450       545  10000  0.00%  0.00%  0.00% 0             GC
0x4b174020       50         5  10000  0.00%  0.00%  0.00% 0 linkscan_user_t
0x4af77020        0         0      0  0.00%  0.00%  0.00% 0 bshell_reaper_t
0x4abcc020        0         0      0  0.00%  0.00%  0.00% 0        tSysLog
0x4ab9f020   107130     10713  10000  0.00%  0.00%  0.00% 0     tTimerTask
0x4ab6f020  3677890    367789  10000  0.00%  0.00%  0.02% 0       tExcTask
0x4ab5f020       20         2  10000  0.00%  0.00%  0.00% 0       tLogTask
0x4ab3e020    68310      6831  10000  0.00%  0.00%  0.00% 0       tUsrRoot
0x40697020      680        68  10000  0.00%  0.00%  0.00% 0           main
0x4c729020        0         0      0  0.00%  0.00%  0.00% 0    poePortScan
0x4c714020   579080     57908  10000  0.00%  0.00%  0.00% 0   l2ProcMwpAck
0x4c6fd020        0         0      0  0.00%  0.00%  0.00% 0 nvProcessMwpAck
0x4c2df020      400        40  10000  0.00%  0.00%  0.00% 0        brAgent
0x4bfc8020   520510     52051  10000  0.00%  0.00%  0.00% 0        nvAgent
0x4bea5020   914880     91488  10000  0.00%  0.00%  0.00% 0        L2Agent
0x4be88020      240        24  10000  0.00%  0.00%  0.00% 0          dsagt
```

```
0x4be4f020        0          0      0  0.00%  0.00%  0.00% 0    ifaDispatch
0x4bc84020  4574350     457435  10000  0.00%  0.50%  0.52% 0        ifagt_1
0x4bb85020    12330       1233  10000  0.00%  0.00%  0.00% 0       aclAgent
0x4bbbb020   277150      27715  10000  0.00%  0.00%  0.00% 0       sflPEAgt
0x4bbb8020   124360      12436  10000  0.00%  0.00%  0.00% 0          count
0x4c765020  1727740     172774  10000  0.00%  0.00%  0.00% 0          PETmr

---------------------------- show process cpu summary --------------------------

CPU utilization        5Sec    1Min    5Min
-----------------------------------------
UNIT1                    1%      0%      0%
UNIT3                    0%      0%      0%

---------------------------------- show system -------------------

Stack MAC                  : f8:b1:56:62:61:08

--  Unit 1 --
Unit Type                  : Management Unit
Status                     : online
Next Boot                  : online
Required Type              : C1048P - 48-port GE
Current Type               : C1048P - 48-port GE
Master priority            : 0
Hardware Rev               : 5.0
Num Ports                  : 52
Up Time                    : 6 day, 21 hr, 13 min
Dell Networking OS Version : 9.9(0.0)
Jumbo Capable              : yes
POE Capable                : yes
FIPS Mode                  : disabled
Burned In MAC              : f8:b1:56:62:61:08
No Of MACs                 : 66

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus   FanSpeed(rpm)
-------------------------------------------------------------------------
  1     0    up           AC      NA          NA
  1     1    absent               NA          NA

--  Fan  Status  --
Unit Bay   TrayStatus  Fan0    Speed   Fan1    Speed
-------------------------------------------------------------------------
1    0     up          up      9056    up      9056

Speed in RPM

--  Unit 3 --
Unit Type                  : Standby Unit
Status                     : online
Next Boot                  : online
Required Type              : C1048P - 48-port GE
Current Type               : C1048P - 48-port GE
Master priority            : 0
Hardware Rev               : 5.0
Num Ports                  : 52
Up Time                    : 6 day, 21 hr, 13 min
Dell Networking OS Version : 9.9(0.0)
Jumbo Capable              : yes
POE Capable                : yes
FIPS Mode                  : disabled
Burned In MAC              : 34:17:eb:00:bb:77
No Of MACs                 : 66

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus   FanSpeed(rpm)
-------------------------------------------------------------------------
  3     0    up           AC      NA          NA
  3     1    down         DC      NA          NA

--  Fan  Status  --
Unit Bay   TrayStatus  Fan0    Speed   Fan1    Speed
-------------------------------------------------------------------------
3    0     up          up      10000   up      10000

Speed in RPM
```

```
---------------------------------- show environment -------------------

--  Fan  Status  --
Unit Bay   TrayStatus  Fan0    Speed   Fan1    Speed
-------------------------------------------------------------------------
1    0     up          up      9056    up      9056
3    0     up          up      10000   up      10000

Speed in RPM

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus   FanSpeed(rpm)
-------------------------------------------------------------------------
  1     0    up           AC      NA          NA
  1     1    absent               NA          NA
  3     0    up           AC      NA          NA
  3     1    down         DC      NA          NA

-- Unit Environment Status  --
Unit  Status        Temp   Voltage
-------------------------------------------------------------------------
* 1   online        38C    ok
  3   online        42C    ok

* Management Unit

--  Thermal Sensor Readings (deg C)  --
Unit  Sensor0  Sensor1  Sensor2
---------------------------------
  1       38       28       41
  3       42       29       47


---------------------------------- show inventory -------------------
System Type            : C1048P
System Mode            : 1.0
Software Version       : 9.9(0.0)

Unit Type  Serial Number  Part Number Rev  Piece Part ID  Rev  Svc Tag  Exprs Svc Code
---------    ------------ ------------------------------ ---------------------
* 1 C1048P-01-1G-48 NA  0J9K8D A01  CN-0J9K8D-28298-4C3-0057 A01 4JBN0Z1 987 553 681 3
  3 C1048P-01-1G-48 NA   7590009701   001  US-0F14T0-77951-3AG-000A 01   NA       NA
  1 C1048P-PWR-AC                                    N/A             N/A  N/A  N/A
  1 C1048P-FAN                                       N/A             N/A  N/A  N/A
  3 C1048P-PWR-AC                                    N/A             N/A  N/A   N/A
  3 C1048P-FAN                                       N/A             N/A  N/A   N/A
* 1 usbflash:      40962316             - 11.00  N/A                 N/A  N/A   N/A

* - Management Unit


Software Protocol Configured
---------------------------------------------------------------
  LLDP


---------------------------------- show lldp neighbors ----------------
Loc PortID   Rem Host Name     Rem Port Id                Rem Chassis Id
-------------------------------------------------------------------------

Te 1/1       -               TenGigabitEthernet 6/12   34:17:eb:00:20:00

---------------------------------- show control-bridge status -----------
Reason: CNU - CSP Not Up, IPE - IPC Program Error
        PPE - PEM Program Error, CPE - CHM Program Error
        UE - UnKnown Error

CB System MAC    : 34:17:eb:00:20:00
Csp Sess Status  : UP
Active CB        : YES
Uplink LAG       : Port-channel 257
LAG Admin Status : UP
LAG Oper Status  : UP
---------------------------------
Status     Reason  RPM-Id  PE-Id
```

```
---------------------------------
Online     -       0       1

---------------------------------- show log --------------------
Syslog logging: enabled
    Console logging: level debugging
    Monitor logging: level debugging
    Buffer logging: level debugging, 54 Messages Logged, Size (40960 bytes)
    Trap logging: level informational
Sep 8 13:07:30: %PE-UNKN-UNIT1-U:CP %IRC-6-IRC_COMMUP: Link to peer
 stack-unit is up
Sep 8 13:07:30: %PE-UNKN-UNIT1-U:CP %RAM-6-ELECTION_ROLE: Stack-unit 1
 is transitioning to Management Stack-unit.
Sep 8 13:07:31: %PE-UNKN-UNIT1-M:CP %CHMGR-5-STACKUNIT_DETECTED:
stack-unit 3 present
Sep 8 13:07:31: %PE-UNKN-UNIT1-M:CP %POLLMGR-2-ALT_STACKUNIT_STATE:
Alternate Stack-unit is present
Sep 8 13:07:31: %PE-UNKN-UNIT1-M:CP %CHMGR-5-STACKUNIT_DETECTED: stack-unit
 1 present
Sep 8 13:07:31: %PE-UNKN-UNIT1-M:CP %CHMGR-5-CHECKIN: Checkin from
stack-unit 1 (type C1048P, 52 ports)
Sep 8 13:07:31: %PE-UNKN-C1048P:1 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 60 % of the full speed
Sep 8 13:07:31: %PE-UNKN-C1048P:1 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
 changed to 75 % of the full speed
Sep 8 13:07:31: %PE-UNKN-UNIT1-M:CP %RAM-5-STACKUNIT_STATE: Stack-unit 1
 is in Active State.
Sep 8 13:07:32: %PE-UNKN-UNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Po 257
Sep 8 13:07:32: %PE-UNKN-UNIT1-M:CP %CHMGR-5-PEM_INSERTED: Power entry
 module 0 of unit 1 is inserted
Sep 8 13:07:32: %PE-UNKN-UNIT1-M:CP %CHMGR-0-PS_UP: Power supply 0 in
unit 1 is up
Sep 8 13:07:32: %PE-UNKN-UNIT1-M:CP %CHMGR-5-PEM_REMOVED: Power entry
module 1 of unit 1 is absent
Sep 8 13:07:32: %PE-UNKN-UNIT1-M:CP %CHMGR-5-FANTRAY_INSERTED: Fan tray 0
of Unit 1 is inserted
Sep 8 13:07:32: %PE-UNKN-UNIT1-M:CP %CHMGR-4-TEMP_STATUS_CHANGE:  Unit 1
temperature state changed
to 1 (Current temperature 40C).
Sep 8 13:07:32: %PE-UNKN-UNIT1-M:CP %SEC-5-LOGIN_SUCCESS: Login successful
 on console
Sep 8 13:07:32: %PE-UNKN-UNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 1/1
Sep 8 13:07:33: %PE-UNKN-UNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 1/2
Sep 8 13:07:33: %PE-UNKN-C1048P:1 %IFAGT-5-STACK_PORT_LINK_UP: Changed
stack port state to up: 1/1
Sep 8 13:07:33: %PE-UNKN-C1048P:1 %IFAGT-5-INSERT_OPTICS_PLUS: Optics SFP+
 inserted in slot 1 port 1
Sep 8 13:07:33: %PE-UNKN-UNIT1-M:CP %CHMGR-5-STACKUNIT_UP: stack-unit 1
is up
Sep 8 13:07:33: %PE-UNKN-UNIT1-M:CP %CHMGR-5-CHECKIN: Checkin from
stack-unit 3 (type C1048P, 52 ports)
Sep 8 13:07:33: %PE-UNKN-UNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 3/1
Sep 8 13:07:33: %PE-UNKN-UNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 3/2
Sep 8 13:07:33: %PE-UNKN-UNIT1-M:CP %CHMGR-5-STACKUNIT_UP: stack-unit3 is up
Sep 8 13:07:33: %PE-UNKN-UNIT1-M:CP %CHMGR-2-SYSTEM_READY: System ready
Sep 8 13:07:34: %PE-UNKN-UNIT1-M:CP %CHMGR-5-PEM_INSERTED: Power entry
module 0 of unit 3 is inserted
Sep 8 13:07:34: %PE-UNKN-UNIT1-M:CP %CHMGR-0-PS_UP: Power supply 0 in unit
 3 is up
Sep 8 13:07:34: %PE-UNKN-UNIT1-M:CP %CHMGR-5-PEM_INSERTED: Power entry
module 1 of unit 3 is inserted
Sep 8 13:07:34: %PE-UNKN-UNIT1-M:CP %CHMGR-0-PS_DOWN: Major alarm: Power
supply 1 in unit 3 is down
Sep 8 13:07:34: %PE-UNKN-C1048P:3 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 60 % of the full speed
Sep 8 13:07:34: %PE-UNKN-UNIT1-M:CP %CHMGR-5-FANTRAY_INSERTED: Fan tray 0
 of Unit 3 is inserted
Sep 8 13:07:34: %PE-UNKN-C1048P:3 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 60 % of the full speed
Sep 8 13:07:34: %PE-UNKN-C1048P:3 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 75 % of the full speed
Sep 8 13:07:35: %PE-UNKN-UNIT1-M:CP %CHMGR-4-TEMP_STATUS_CHANGE:  Unit 3
```

```
temperature state changed
o 1 (Current temperature 44C).
Sep 8 13:07:35: %PE-UNKN-C1048P:3 %IFAGT-5-STACK_PORT_LINK_UP: Changed stack
 port state to up: 3/1
Sep 8 13:07:35: %PE-UNKN-C1048P:3 %IFAGT-5-INSERT_OPTICS_PLUS: Optics SFP+
 inserted in slot 3 port 1
Sep 8 13:07:35: %PE-UNKN-C1048P:3 %IFAGT-5-INSERT_OPTICS_PLUS: Optics
SFP+ inserted in slot 3 port 2
Sep 8 13:07:35: %PE-UNKN-UNIT1-M:CP %IFMGR-5-OSTATE_UP: Changed interface
state to up: Te 3/1
Sep 8 13:07:35: %PE-UNKN-UNIT1-M:CP %IFMGR-5-OSTATE_UP: Changed interface
 state to up: Po 257
Sep 8 13:07:39: %PE255-UNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 2/1
Sep 8 13:07:39: %PE255-UNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 2/2
Sep 8 13:07:40: %PE255-UNIT1-M:CP %EVL-6-EVENT_LOGGING: Start uploading
pre-recorded traps(count:24) to CB
Sep 8 13:07:40: %PE255-UNIT1-M:CP %EVL-6-EVENT_LOGGING: Completed
uploading pre-recorded traps(send count:24,
pending traps:0) to CB
Sep 8 13:07:53: %PE-UNKN-UNIT3-S:CP %RAM-5-STACKUNIT_STATE: Stack-unit 3
 is in Standby State.
Sep 8 13:07:54: %PE255-UNIT3-S:CP %EVL-6-EVENT_LOGGING: Start uploading
pre-recorded traps(count:9) to CB
Sep 8 13:07:54: %PE255-UNIT3-S:CP %EVL-6-EVENT_LOGGING: Completed uploading
pre-recorded traps(send count:9,
pending traps:0) to CB
Sep 8 13:08:03: %PE255-C1048P:3 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 85 % of the full speed
Sep 8 13:08:04: %PE255-UNIT1-M:CP %CHMGR-4-TEMP_STATUS_CHANGE:  Unit 3
temperature state changed to 2 (Current temperature 50C).
Sep 10 14:44:06: %PE255-UNIT1-M:CP %SEC-5-LOGOUT: Exec session is terminated
 on console
Sep 10 15:20:45: %PE255-UNIT1-M:CP %IFMGR-5-OSTATE_UP: Changed interface
state to up: Te 1/1
Sep 10 15:20:50: %PE255-UNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 0/1
Sep 10 15:20:50: %PE255-UNIT1-M:CP %IFMGR-5-ASTATE_UP: Changed interface
Admin state to up: Te 0/2
Sep 17 11:39:00: %PE1-UNIT1-M:CP %SEC-5-LOGIN_SUCCESS: Login successful for
user peadmin on line vty0 ( internal Ipa )
Dell#
```

Related Commands

- show version — displays the Dell Networking OS version.
- show system — displays the current switch status.
- show environment — displays the system component status.

show util-threshold cpu

Display the utilization thresholds of switch CPUs.

C9000 Series

Syntax `show util—threshold cpu`

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series, E-Series, S25 and S50.

Usage Information Use the `show util-threshold cpu` command to display the CPU utilization thresholds used to send SNMP traps. When the switch CPUs exceed the configured time to process packets or data, a threshold notification is sent as an SNMP trap. To reconfigure the currently configured values, use the `util-threshold cpu` command.

Example

```
Dell#show util-threshold cpu

Processor              5Sec        1Min        5Min
                      High   Low  High   Low  High   Low
=============================================================
CP                    0      0    85     75     80     70
RP                    0      0    85     75     80     70
LP 0                  0      0    85     75     80     70
LP 1                  0      0    85     75     80     70
LP 2                  0      0    85     75     80     70
LP 3                  0      0    85     75     80     70
LP 4                  0      0    85     75     80     70
LP 5                  0      0    85     75     80     70
LP 6                  0      0    85     75     80     70
LP 7                  0      0    85     75     80     70
LP 8                  0      0    85     75     80     70
LP 9                  0      0    85     75     80     70
LP 10                 0      0    85     75     80     70
LP 11                 0      0    85     75     80     70
PE                    0      0    85     75     80     70
```

Related Commands

- util-threshold cpu – Configure CPU utilization thresholds.
- util-threshold mem – Configure memory utilization thresholds.

show util-threshold memory

Display the memory utilization thresholds of switch CPUs.

C9000 Series

Syntax `show util—threshold memory`

Defaults None

Command Modes EXEC Privilege

Command History

Version	Description
9.9 (0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series, E-Series, S25 and S50.

Usage Information

Use the `show util-threshold memory` command to display the memory utilization thresholds used to send SNMP traps. When switch CPUs exceed the configured (high or low) memory percentage to process packets or data, a threshold notification is sent as an SNMP trap. To reconfigure the currently configured values, use the `util-threshold memory` command.

Example

```
Dell#show util-threshold memory

Processor           High     Low
================================
CP                   92      82
RP                   92      82
LP 0                 92      82
LP 1                 92      82
LP 2                 92      82
LP 3                 92      82
LP 4                 92      82
LP 5                 92      82
LP 6                 92      82
LP 7                 92      82
LP 8                 92      82
LP 9                 92      82
LP 10                92      82
LP 11                92      82
PE                   92      82
```

Related Commands

- util-threshold mem – Configure memory utilization thresholds.
- util-threshold cpu – Configure CPU utilization thresholds.

show version

Display the current Dell Networking OS version information on the system.

C9000 Series

Syntax

`show version [all |[pe` *`pe-id`*`]`

From a **PE console**, use `show version` to view the software version information.

Parameters

all	Enter the keyword `all` to view all components.
pe *pe-id*	Enter the keyword `pe` and the port extender (PE) ID to view show version output for a specific PE. The PE ID range is from 0 to 255.

NOTE: The pe option is only available when the extended bridge feature is enabled.

.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information The following table lists the information shown in the example.

Lines Beginning With	Lines Beginning With
Dell Force10 Network...	Name of the operating system
Dell Force10 Operating...	OS version number
Dell Force10 Application...	Software version
Copyright (c)...	Copyright information
Build Time...	Software build's date stamp
Build Path...	Location of the software build files loaded on the system
Dell Force10 uptime is...	Amount of time the system has been up
System image...	Image file name
Chassis Type:	Chassis type (for example, E1200, E600, E600i, E300, C300, C150, S25, S50, S55, S60, S4810)
Control Processor:...	Control processor information and amount of memory on processor
Route Processor 1:...	Route processor 1 information and the amount of memory on that processor
Route Processor 2:...	Route processor 2 information and the amount of memory on that processor
128K bytes...	Amount and type of memory on system

Lines Beginning With	Lines Beginning With
1 Route Processor...	Hardware configuration of the system, including the number and type of physical interfaces available

Example

```
Dell#show version
Dell Real Time Operating System Software
Dell Operating System Version: 2.0
Dell Application Software Version: 1-0(0-4095)
Copyright (c) 1999-2015 by Dell Inc. All Rights Reserved.
Build Time: Thu Jun 25 18:00:00 2015
Build Path: /build/build01/SW/SRC
Dell Networking OS uptime is 1 hour(s), 0 minute(s)
System image file is "system://A"
System Type: C9010
Control Processor: Intel Rangeley with 2 Gbytes (2127536128 bytes) of memory,
core(s) 2.
Route Processor: Intel Rangeley with 2 Gbytes (2127536128 bytes) of memory,
core(s) 2.
16G bytes of boot flash memory.
2 Route Processor Module.
3 24-port TE/GE
3 24-port TE/GE
4 6-port TE/FG
2 4-port TE/GE
200 Ten GigabitEthernet/IEEE 802.3 interface(s)
12 Forty GigabitEthernet/IEEE 802.3 interface(s)
```

Example: show version all

```
Dell#show version all
Dell Real Time Operating System Software
Dell Operating System Version:  2.0
Dell Application Software Version:  1-0(0-4079)
Copyright (c) 1999-2015 by Dell Inc. All Rights Reserved.
Build Time: Mon Jun 22 06:00:00 2015
Build Path: /build/build01/SW/SRC
Dell Networking OS uptime is 1 hour(s), 36 minute(s)

System image file is "pt-c9000-2"

System Type: C9010
Control Processor: Intel Rangeley with 2 Gbytes (2127536128 bytes) of memory,
core(s) 2.

Route Processor: Intel  Rangeley with 2 Gbytes (2127536128 bytes) of memory,
core(s) 2.

16G bytes of boot flash memory.

  2 Route Processor Module.
  3 24-port TE/GE
  3 24-port TE/GE
  3 6-port TE/FG
  2 4-port TE/GE
176 Ten GigabitEthernet/IEEE 802.3 interface(s)
12 Forty GigabitEthernet/IEEE 802.3 interface(s)

PE-ID: 0
----------

Dell Real Time Operating System Software
Dell Operating System Version:  2.0
Dell Application Software Version:  1-0(0-4079)
Copyright (c) 1999-2015 by Dell Inc. All Rights Reserved.
Build Time: Mon Jun 22 06:00:00 2015
Build Path: /build/build01/SW/SRC
Dell Networking OS uptime is 1 hour(s), 28 minute(s)
```

```
System image file is "system://B"

System Type: C1048P
Control Processor: Broadcom 56340 (ver A0) with 1 Gbytes (1073741824 bytes) of
memory, cores(s) 1.

16G bytes of boot flash memory.

  4 48-port GE (VE)
192 GigabitEthernet/IEEE 802.3 interface(s)

PE-ID: 100
----------

Dell Real Time Operating System Software
Dell Operating System Version:  2.0
Dell Application Software Version:  1-0(0-4079)
Copyright (c) 1999-2015 by Dell Inc. All Rights Reserved.
Build Time: Mon Jun 22 06:00:00 2015
Build Path: /build/build01/SW/SRC
Dell Networking OS uptime is 1 hour(s), 29 minute(s)
System image file is "system://B"

System Type: C1048P
Control Processor: Broadcom 56340 (ver A0) with 1 Gbytes (1073741824 bytes) of
memory, cores(s) 1.

16G bytes of boot flash memory.

  2 48-port GE (VE)
96 GigabitEthernet/IEEE 802.3 interface(s)
```

Example: show version (PE Console)

```
Dell#show version
Dell Real Time Operating System Software
Dell Operating System Version:  2.0
Dell Application Software Version:  1-0(0-4092)
Copyright (c) 1999-2015 by Dell Inc. All Rights Reserved.
Build Time: Thu Jun 25 09:00:00 2015
Build Path: /build/build01/SW/SRC
Dell Networking OS uptime is 2 week(s), 0 day(s), 3 hour(s), 35 minute(s)

System image file is "system://A"

System Type: C1048P
Control Processor: Broadcom 56340 (ver A0) with 1 Gbytes (1073741824 bytes) of
memory, core(s) 1.

16G bytes of boot flash memory.

  1 48-port GE (VE)
 48 GigabitEthernet/IEEE 802.3 interface(s)
```

telnet

Connect through Telnet to a server. The Telnet client and server in the Dell Networking OS support IPv4 and IPv6 connections. You can establish a Telnet session directly to the router or a connection can be initiated from the router.

C9000 Series

Syntax

```
telnet {host | ip-address | ipv6-address prefix-length | vrf vrf instance name}
[/source-interface]
```

Parameters

host	Enter the name of a server.
ip-address	Enter the IPv4 address in dotted decimal format of the server.
ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
source-interface	(OPTIONAL) Enter the keywords `/source-interface` then the interface information to include the source interface. Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from zero (0) to 16383. • For the Null interface, enter the keyword `null` then 0. • For a Port Channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128. • For Tunnel interface types, enter the keyword `tunnel` then the slot/ port information. The range is from 1 to 16383. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9 (0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810. Added support for *source-interface* for link-local IPv6 addressing.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced on the E-Series ExaScale (IPv6). Increased the number of VLANs on ExaScale to 4094 (was 2094).
8.1.1.0	Introduced on the E-Series ExaScale (IPv4).
7.9.1.0	Introduced VRF.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series and added support for IPv6 address on the E-Series only.

terminal length

Configure the number of lines displayed on the terminal screen.

C9000 Series

Syntax `terminal length screen-length`

Parameters

screen-length	Enter a number of lines. Entering zero causes the terminal to display without pausing. The range is from 0 to 512.

Defaults 24 lines

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

traceroute

View a packet's path to a specific device.

C9000 Series

Syntax

```
traceroute {host | vrf instance | ip-address | ipv6-address}
```

Parameters

host	Enter the name of device.
vrf instance	(Optional) E-Series Only: Enter the keyword `vrf` then the VRF Instance name.
ip-address	Enter the IP address of the device in dotted decimal format.
ipv6-address	Enter the IPv6 address, in the x:x:x:x::x format, to which you are testing connectivity. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**

Defaults

- Timeout = **5 seconds**
- Probe count = **3**
- 30 hops max
- 40 byte packet size
- UDP port = **33434**

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced on the E-Series ExaScale with IPv6.
8.1.1.0	Introduced on the E-Series ExaScale (IPv4 only).
7.9.1.0	Introduced VRF.
7.6.1.0	Added support for the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
7.4.1.0	Added support for IPv6 address on the E-Series.
E-Series	Original command.

Usage Information

When you enter the `traceroute` command without specifying an IP address (Extended Traceroute), you are prompted for a target and source IP address, timeout (in seconds) (default is **5**), a probe count (default is **3**), minimum TTL (default is **1**), maximum TTL (default is **30**), and port number (default is **33434**). To keep the default setting for those parameters, press the ENTER key.

For IPv6, you are prompted for a minimum hop count (default is **1**) and a maximum hop count (default is **64**).

Example (IPv4)

```
Dell#traceroute www.force10networks.com

Translating "www.force10networks.com"...domain server (10.11.0.1) [OK]
Type Ctrl-C to abort.

------------------------------------------------
Tracing the route to www.force10networks.com (10.11.84.18),
30 hops max, 40 byte packets
------------------------------------------------

TTL Hostname      Probe1     Probe2     Probe3
1   10.11.199.190 001.000 ms 001.000 ms 002.000 ms
2   gwegress-sjc-02.force10networks.com (10.11.30.126) 005.000 ms 001.000 ms
001.000 ms
3   fw-sjc-01.force10networks.com (10.11.127.254) 000.000 ms 000.000 ms
000.000 ms
4   www.force10networks.com (10.11.84.18) 000.000 ms 000.000 ms 000.000 ms
Dell#
```

Example (IPv6)

```
Dell#traceroute 100::1

Type Ctrl-C to abort.

------------------------------------------------
Tracing the route to 100::1, 64 hops max, 60 byte packets
------------------------------------------------
Hops Hostname Probe1    Probe2    Probe3
1    100::1 000.000 ms 000.000 ms 000.000 ms

Dell#traceroute 3ffe:501:ffff:100:201:e8ff:fe00:4c8b

Type Ctrl-C to abort.

------------------------------------------------
Tracing the route to 3ffe:501:ffff:100:201:e8ff:fe00:4c8b,
64 hops max, 60 byte packets
------------------------------------------------
Hops Hostname  Probe1   Probe2    Probe3
 1  3ffe:501:ffff:100:201:e8ff:fe00:4c8b
             000.000 ms 000.000 ms 000.000 ms
Dell#
```

Related Commands

ping — tests the connectivity to a device.

undebug all

Disable all debug operations on the system.

C9000 Series

Syntax `undebug all`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

upload trace-log

Upload a trace log file from a switch CPU.

C9000 Series

Syntax `upload trace-log {cp [cmd-history]| linecard | slot-id | pe pe-id [stack-unit unit number ] |rp } [sw-trace | hw-trace]`

Parameters

rp	Enter the keyword `rp` to upload a trace log from the Route Processor.
cp	Enter the keyword `cp` to upload a trace log from the Control Processor.
linecard *slot-id*	Enter the `linecard slot-id` parameters to specify the line-card CPU whose trace log you want to upload.

cmd-history	Enter the keyword `cmd-history` to upload the command history from the specified CPU.
hw-trace	Enter the keyword `hw-trace` to upload the hardware trace log from the specified CPU.
sw-trace	Enter the keyword `sw-trace` to upload the software trace log from the specified CPU.
pe *pe-id*	Enter the keyword `pe` and port extender ID. Range is from 0 to 255. **NOTE: The pe option is only available when the extended bridge feature is enabled.**
stack *unit number*	Enter the keyword `stack unit` and a stack unit number. Stack unit range is from 0 to 7.

Defaults None.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.

Usage Information Trace log information is uploaded to `flash:/TRACE_LOG_DIR`

In a dual homing setup, you can use this command only from the primary VLT peer.

util-threshold cpu

Configure the high or low CPU utilization thresholds for SNMP traps.

C9000 Series

Syntax
```
util—threshold cpu {5sec | 1min | 5min} {all | cp |lp slot-id | pe | rp} {high {0-100} | low {0-100}}
```

Parameters

cpu-utilization-time Enter one of the following values to configure the threshold level for the time in which a switch CPU can be used:

- 5 sec
- 1 min
- 5 min

cp	Enter the keyword `cp` to configure the CPU utilization time for the Control Processor CPU.
rp	Enter the keyword `rp` to configure the CPU utilization time for the Route Processor CPU.
lp *slot-id*	Enter the keyword `lp` and the linecard processor (lp) *slot-id* for which you want to configure the CPU utilization time. The range for `lp` *slot-id* is from 0 to 11.
pe	Enter the keyword`pe` to configure the CPU utilization time for port extenders (PE) configured in the system. Range is from 0 to 255. **NOTE: The pe option is only available when the extended bridge feature is enabled.**
all	Enter the keyword `all` to configure the CPU utilization time on all switch CPUs: Control Processor, Route Processor, port extender (PE) and line cards.
{{high | low} *cpu-utilization-threshold-percentage*}	Enter a percentage value to configure the high or low threshold level for the time in which a switch CPU can be used. The percentage of CPU use ranges from 0 to 100. **NOTE: A threshold level of 0 disables Syslog and SNMP traps.**

Defaults

- High CPU utilization threshold: 1 min = 85%, 5 min = 80%
- Low CPU utilization threshold: 1 min = 75%, 5 min = 70%

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information

When the total CPU utilization exceeds the configured threshold for the specified time, a threshold notification is sent as an SNMP trap. If a low threshold value is not specified, the low threshold value is set to the same value as the high threshold value. The system generates a Syslog and SNMP trap each time the configured CPU threshold is crossed.

Use this command in Configuration Terminal Batch mode to configure the CPU utilization thresholds in a dual-homing setup.

NOTE: The 5 sec `util-threshold cpu` command is disabled by default on all switches. To enable the command, enter `util-threshold cpu 5sec all high` {value greater than zero}. To disable the Syslog and traps for the 5 sec CPU utilization thresholds, enter `util-threshold cpu 5sec all high 0` or `no util-threshold cpu 5sec {all | cp | lp` *slot-id* `| pe | rp }`.

Example

```
Dell(conf)# util-threshold cpu 5sec cp high 50
```

In this example, the low threshold value is not specified so the system takes the value set for the high threshold value. In all other cases, the low threshold value must be equal to or less than the high threshold value.

Related Commands

- show util-threshold cpu – Display the configured values of CPU utilization thresholds.
- show util-threshold memory – Display the configured values of memory utilization thresholds.

util-threshold memory

Configure the high or low memory utilization thresholds for SNMP traps.

C9000 Series

Syntax

```
util—threshold memory {all | cp | lp slot-id | pe | rp [high {0-100} | low {0-100}]}
```

Parameters

all	Enter the keyword `all` to configure the memory utilization threshold on all switch CPUs: Control Processor, Route Processor, line cards, and port extenders (PE).
cp	Enter the keyword `cp` to configure the memory utilization threshold for the Control Processor CPU.
lp *slot-id*	Enter the keyword `lp` and the linecard processor (lp) *slot-id* for which you want to configure the CPU utilization time. The range for `lp` *slot-id* is from 0 to 11.
pe	Enter the keyword`pe` to configure the CPU utilization time for port extenders (PE) configured in the system. **NOTE: The pe option is only available when the extended bridge feature is enabled.**
rp	Enter the keyword `rp` to configure the memory utilization threshold for the Route Processor CPU.
{{high | low} *cpu-utilization-threshold-percentage*}	Enter a percentage value to configure the high or low threshold level for the percentage of memory a switch CPU can use. The percentage of memory utilization ranges from 0 to 100. **NOTE: A threshold level of 0 disables Syslog and SNMP traps.**

Default

- High threshold: 92%
- Low threshold: 82%

Command Mode

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information

When the total memory utilization for a CPU exceeds the configured high/low threshold for a given time, a threshold notification is sent as an SNMP trap. If a low threshold value is not specified, the low threshold value is set to the same value as the high threshold value.

To return the memory thresholds to the default values, enter the `no util-threshold mem all | cp | lp slot-id | pe | rp` command.

Use this command in Configuration Terminal Batch mode to configure the memory utilization thresholds in a dual-homing setup.

Example cp

```
Dell(conf)# util-threshold memory cp high 75 low 67
```

Example pe

```
Dell(conf)# util-threshold memory pe high 85 low 70
```

Related Commands

- show util-threshold memory – Display the configured values of memory utilization thresholds.
- show util-threshold cpu – Display the configured values of CPU utilization thresholds.

virtual-ip

Configure a virtual IP address for the active management interface. You can configure virtual addresses both for IPv4 and IPv6 independently.

C9000 Series

Syntax

`virtual-ip {ipv4-address | ipv6-address}`

To return to the default, use the `no virtual-ip {ipv4-address | ipv6-address}` command.

Parameters

ipv4-address	Enter the IP address of the active management interface in a dotted decimal format (A.B.C.D.).
ipv6-address	Enter an IPv6 address of the active management interface, in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

You can configure both IPv4 and IPv6 virtual addresses simultaneously, but only one of each. Each time this command is issued, it replaces the previously configured address of the same family, IPv4 or IPv6. The `no virtual-ip` command takes an address/prefix-length argument, so that the desired address only is removed. If you enter the `no virtual-ip` command without any specified address, then both IPv4 and IPv6 virtual addresses are removed.

Related Commands

ip address — assigns a primary and secondary IP address to the interface.

write

Copy the current configuration to either the startup-configuration file or the terminal.

C9000 Series

Syntax

```
write {memory | terminal}
```

Parameters

memory	Enter the keyword `memory` to copy the current running configuration to the startup configuration file. This command is similar to the `copy running-config startup-config` command.
terminal	Enter the keyword `terminal` to copy the current running configuration to the terminal. This command is similar to the `show running-config` command.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

The `write memory` command saves the running-configuration to the file labeled startup-configuration. When using a LOCAL CONFIG FILE other than the startup-config not named “startup-configuration,” the running-config is not saved to that file.

4

File Management

This chapter contains command line interface (CLI) commands needed to manage the configuration files as well as other file management commands.

The commands in this chapter are supported by the Dell Networking OS on the C9000 switch.

Topics:

- boot system
- cd
- copy
- delete
- dir
- format flash
- mkdir
- mount nfs
- pwd
- rename
- restore factory-defaults
- rmdir
- show boot bmp
- show boot system
- show bootvar
- show file
- show file-systems
- show os-version
- show running-config
- show startup-config
- upgrade
- upgrade system-image-os6
- verify

boot system

Specify the location where the Dell Networking OS image used to boot the system is stored.

C9000 Series

Syntax

```
boot system [gateway ip address | [rpm0 {default | primary |secondary [ftp: |
system:{A:| B:} | tftp:] }] [rpm1 {default | primary | secondary [ftp: |system:
{A:|B:} | tftp:]}]
```

Parameters

gateway	Enter the IP address of the default next-hop gateway for the management subnet.
ip-address	Enter an IP address in dotted decimal format.
rpm0	Enter the keyword `rpm0` to specify the route processor module 0.
rpm1	Enter the keyword `rpm1` to specify the route processor module 1.
default	Enter the keyword `default` to use the default Dell Networking OS image.
primary	Enter the keyword `primary` to use the primary Dell Networking OS image.
secondary	Enter the keyword `secondary` to use the secondary Dell Networking OS image.
ftp:	Enter the keyword `FTP:` to retrieve the image from an FTP server: ftp:*//userid:password @host-ip/filepath*.
system *A:* | *B:*	Enter `A:` or `B:` to boot one of the flash system partitions.
tftp:	Enter the keyword `TFTP:` to retrieve the image from a TFTP server: tftp:*//host-ip/filepath*.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Usage Information To display these changes in the `show bootvar` command output, save the running configuration to the startup configuration (using the `copy` command) and reload the system.

To specify the IP address of the default next-hop gateway for the management subnet, use the `boot system gateway` command.

Related Command show boot system — Displays information about boot images currently stored on the system.

cd

Change to a different working directory.

C9000 Series

Syntax `cd {flash: directory name/path | usbflash directory name/path}`

From a **PE console**, use `cd {flash: directory name/path | usbflash directory name/path }` to change to a different working irectory.

Parameters

directory	(OPTIONAL) Enter one of the following: • `flash:` (internal flash) or any sub-directory • `nfsmount://<mount-point>/filepath:` NFS-mounted path **NOTE: While switching to a remote NFS file system, it is mandatory to specify the mount-point that indicates the working directory on the NFS file system. You cannot enter the root directory of the remote NFS file system.** • `usbflash:` (USB Flash) or any sub-directory
flash: *([[flash://]directory_path])*	Enter the internal directory name and the directory path.
usbflash: *([[usbflash://]directory_path])*	Enter the USB flash directory name and the directory path.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added the `nfsmount:<mount-point>` parameters to support remote NFS file system.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information You can also use the `cd {flash: directory name/path | usbflash directory name/path}` command from a port extender (PE) console to change the working directory.

Example

```
Dell#cd flash://TRACE_LOG_DIR
```

copy

Copy one file to another location. Dell Networking OS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP (in the *hostip* field).

C9000 Series

Syntax

`copy compressed-config` *`source-filename destination-filename`*

From a **PE console**, use `copy flash:` [*`source-filename destination-filename`*] | `usbflash:` [*`source-filename destination-filename`*]

Parameters

Enter the following location keywords and information:

compressed-config Enter the keyword `compressed-config` to copy one file, after optimizing and reducing the size of the configuration file, to another location. Dell Networking OS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP (in the hostip field).

file-name

To copy a file from the internal FLASH	enter `flash://` and then the filename
To copy a file on an FTP server	enter `ftp://user:password@hostip/filepath`
To copy a file on an HTTP server	enter `http:` `http://hostip/filepath`
To copy a file on a NFS-mounted system	enter `nfsmount://<mount-point/filepath` **NOTE: While switching to a remote NFS file system, it is mandatory to specify the mount-point that indicates the working directory on the NFS file system. You cannot enter the root directory of the remote NFS file system.**
To copy the running configuration	enter the keyword `running-config`
To copy the startup configuration	enter the keyword `startup-config`
To copy using a Secure Copy (SCP),	enter the keyword `scp:` • If you enter `scp:` in the source position, enter the target URL; • If you enter `scp:` in the target position, first enter the source URL;
To copy a file on a TFTP server	enter `tftp://hostip/filepath`

To copy a file from an external USB drive	enter `usbflash://filepath`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Introduced on N20xx and N30xx series.
9.9(0.0)	Introduced on the C9010 and C1048P.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added the `nfsmount:<mount-point>` parameters to support remote NFS file system.
9.4(0.0)	Added the compressed-config parameter.
9.0.2.0	Introduced on the S6000.
8.4.1.0	Added IPv6 addressing support for FTP, TFTP, and SCP.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added `usbflash` and `rpm0usbflash` commands on E-Series ExaScale.
7.6.1.0	Introduced on the S-Series and added the SSH port number to the SCP prompt sequence on all systems.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information Dell Networking OS supports a maximum of 100 files at the root directory level, on both the internal and external Flash.

When copying a file to a remote location (for example, using Secure Copy [SCP]), enter only the keywords and Dell Networking OS prompts you for the rest of the information. For example, when using SCP, you can enter `copy running-config scp:` where `running-config` is the source and the target is specified in the ensuing prompts. Dell Networking OS prompts you to enter any required information, as needed for the named destination — remote destination, destination filename, user ID, password, etc.

When you use the `copy running-config startup-config` command to copy the running configuration to the startup configuration file, Dell Networking OS creates a backup file on the internal flash of the startup configuration.

When you load the startup configuration or a configuration file from a network server such as TFTP to the running configuration, the configuration is added to the running configuration. This does not replace the existing running configuration. Commands in the configuration file has precedence over commands in the running configuration.

Dell Networking OS supports copying the running-configuration to a TFTP server, an FTP server, or a remote NFS file system. For example:

- `copy running-config tftp:`
- `copy running-config ftp:`
- `copy running-config nfsmount://<mount-point>/filepath`

You can compress the running configuration by grouping all the VLANs and the physical interfaces with the same property. Support to store the operating configuration to the startup config in the compressed mode and to perform an image downgrade without any configuration loss are provided.

Two existing exec mode CLIs, `show running-config compressed` and `write memory compressed` are enhanced to display and store the running configuration in the compressed mode.

From the PE console, you can copy a file to another location using the `copy flash:` *`source-filename destination-filename`*. Similarly, you can use the `copy usbflash:` *`source-filename destination-filename`* command to copy a file from the external USB flash to another location.

Example

In the following `copy scp: flash:` example, `SCP` in the first position indicates that the target is to be specified in the ensuing prompts. Entering `flash:` in the second position indicates that the target is the internal Flash. The source is on a secure server running SSH, so you are prompted for the user datagram protocol (UDP) port of the SSH server on the remote host.

```
Dell#copy running-config scp:/
Address or name of remote host []: 10.10.10.1
Destination file name [startup-config]? old_running
User name to login remote host? sburgess
Password to login remote host? dilling
```

Example

```
Dell#copy running-config nfsmount://<mount-point>/filepath
Destination file name [test.txt]:
User name to login remote host: usrname
Password to login remote host:
```

Example

```
Dell#copy scp: flash:
Address or name of remote host []: 10.11.199.134
Port number of the server [22]: 99
Source file name []: test.cfg
User name to login remote host: admin
Password to login remote host:
Destination file name [test.cfg]: test1.cfg
```

Example

```
Dell#copy compressed-config compressed-cfg
!
6655 bytes successfully copied
Dell#
Dell#copy compressed-config ftp:
Address or name of remote host []: 10.11.8.12
Destination file name [startup-config]:
User name to login remote host: spbalaji
Password to login remote host:
!
6655 bytes successfully copied
```

```
Dell#copy tftp: flash:
Address or name of remote host []: 1.1.1.1
Source file name []: Test
Destination file name [Test]:
```

Example (PE Console)

```
Dell# copy flash://Diag_Test_Report_SU_1.txt flash://PE255_Report.txt
!
19705 bytes successfully copied
```

Related Commands cd– changes the working directory.

delete

Delete a file from the flash. After deletion, files cannot be restored.

C9000 Series

Syntax `delete` *`flash-url`* `[no-confirm]`

From a **PE console**, use `delete {flash:` *`file name/path`* `| usbflash` *`file name/path`*`[no-confirm]}`

Parameters

flash-url	Enter the following location and keywords: • For a file or directory on the internal Flash, enter `flash://` followed by the filename or directory name. • For a file or directory on the NFS mounted file system, enter `nfsmount://` followed by the mount point and the file path. **NOTE: While deleting a file directory on a remote NFS file system, it is mandatory to specify the mount-point that indicates the working directory on the NFS file system. You cannot delete the root directory of the remote NFS file system.** • For a file or directory on an external USB drive, enter `usbflash://` followed by the filename or directory name.
flash: *([[flash://]directory_path])*	Enter the internal file name and the file path.
usbflash: *([[usbflash://]directory_path])*	Enter the USB flash file name and the file path.
no-confirm	(OPTIONAL) Enter the keyword `no-confirm` to specify that Dell Networking OS does not require user input for each file prior to deletion.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.

Version	Description
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added the`nfsmount:<mount-point>` parameters to support remote NFS file system.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

You can also use the `delete {flash: file name/path | usbflash file name/path}` command from a port extender (PE) console to delete a file from the flash or USB flash.

Example

```
Dell#dir flash:
Directory of flash:
1 drwx 4096 Jan 01 1980 00:00:00 +00:00 .
2 drwx 1536 Jun 25 2015 20:58:14 +00:00 ..
3 drwx 4096 Mar 12 2015 05:15:48 +00:00 CORE_DUMP_DIR
4 d--- 4096 Mar 12 2015 05:15:50 +00:00 ADMIN_DIR
5 drwx 4096 Jun 04 2015 01:33:02 +00:00 TRACE_LOG_DIR
6 drwx 4096 Jun 04 2015 01:33:04 +00:00 CONFD_LOG_DIR
7 drwx 4096 Jun 04 2015 01:33:08 +00:00 RUNTIME_PATCH_DIR
8 -rwx 749 Jun 25 2015 23:38:16 +00:00 startup-config
flash: 100450304 bytes total (100409344 bytes free)
```

```
Dell#dir usbflash:
Directory of usbflash:
1 drwx 4096 Jan 01 1980 00:00:00 +00:00 .
2 drwx 1536 Jun 25 2015 20:25:40 +00:00 ..
3 -rwx 8388608 Jun 25 2015 14:54:52 +00:00 50mb
usbflash: 3996688384 bytes total (3988295680 bytes free)
```

dir

Display the files in a file system.

C9000 Series

Syntax

`dir [filename | directory name:]`

From a **PE console**, use `dir {flash:filename/path | usbflash: filename/path }`

Parameters

***filename* | *directory name*:** (OPTIONAL) Enter one of the following:

- For a file or directory on the internal Flash, enter `flash://` then the filename or directory name.

- For a file or directory on an NFS mounted file system, enter `nfsmount://` followed by the mount point and file path.

  NOTE: While displaying a file directory on a remote NFS file system, it is mandatory to specify the mount-point that indicates the working directory on the NFS file system. You cannot display details corresponding to the root directory of the remote NFS file system.

- For a file or directory on the external Flash, enter `usbflash://` then the filename or directory name.

flash: | usbflash:

For PE Console.

Enter one of the following:

- For a directory or file on the internal Flash, enter `flash://` then the directory name or filename and the path.
- For a directory or file on the external Flash, enter `usbflash://` then the directory name or filename and the path.

Defaults

The default is the current directory.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added the `nfsmount:<mount-point>` parameters to support remote NFS file system.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Example

```
Dell#dir
Directory of flash:

  1  drwx       8192   Jan 01 1980 00:00:00 +00:00 .
  2  drwx       3072   Dec 15 2014 06:27:10 +00:00 ..
  3  drwx       4096   Jan 01 1980 00:02:44 +00:00 TRACE_LOG_DIR
  4  drwx       4096   Jan 01 1980 00:02:44 +00:00 CORE_DUMP_DIR
  5  d---       4096   Jan 01 1980 00:02:44 +00:00 ADMIN_DIR
  6  drwx       4096   Jan 01 1980 00:02:44 +00:00 RUNTIME_PATCH_DIR
  7  drwx       4096   Nov 06 2014 06:57:06 +00:00 CONFIG_TEMPLATE
  8  -rwx       4625   Nov 06 2014 06:55:28 +00:00 startup-config
```

```
  9  drwx       4096   May 31 2013 02:49:46 +00:00 CONFD_LOG_DIR
flash: 2056916992 bytes total (2052784128 bytes free)
```

Example (NFS Mount)

```
Dell#dir nfsmount:
Directory of nfsmount:

  1  drwx        512   Nov 06 2014 06:58:19 +00:00 .
  2  drwx        512   Nov 06 2014 06:58:19 +00:00 ..

nfsmount: 1463410688 bytes total (618045440 bytes free)
```

Example (PE Console)

```
Dell#dir
Directory of flash:

  1  drwx       4096   Jan 01 1980 00:00:00 +00:00 .
  2  drwx       1536   Jun 23 2015 06:07:25 +00:00 ..
  3  drwx       4096   Jun 01 2015 19:37:48 +00:00 TRACE_LOG_DIR
  4  drwx       4096   Jun 01 2015 19:37:52 +00:00 CONFD_LOG_DIR
  5  drwx       8192   Jun 01 2015 19:37:52 +00:00 CORE_DUMP_DIR
  6  d---       4096   Jun 01 2015 19:37:56 +00:00 ADMIN_DIR
  7  drwx       4096   Jun 01 2015 19:38:00 +00:00 RUNTIME_PATCH_DIR
  8  -rwx      19705   Jun 08 2015 23:41:44 +00:00 Diag_Test_Report_SU_1.txt

flash: 100450304 bytes total (99524608 bytes free)
```

Related Commands cd – changes the working directory.

format flash

Erase all existing files and reformat the file system in the internal flash memory or the USB drive. After the file system is formatted, files cannot be restored.

C9000 Series

Syntax

```
format {flash: | usbflash:}
```

From a **PE console**, use `format {flash:`*`filename/path`*` | usbflash:`*` filename/path`*` }`

Parameters

flash: | usbflash:

- `flash:` reformat the file system in the internal flash memory.
- `usbflash:` reformat the file system in the USB flash drive.

Defaults **flash memory**

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.11.1	Introduced on the Z9000.

Usage Information

Include the colon (:) when entering this command.

> **CAUTION: This command deletes all files, including the startup configuration file. So, after executing this command, consider saving the running config as the startup config (use the `write memory` command or `copy run start` command).**

You can also use the `format` command from the port extender (PE) console to erase all files from the flash or USB flash.

mkdir

Create a directory on the NFS mounted file system.

C9000 Series

Syntax `mkdir nfsmount://mount-point/usrname`

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced this command.

Example

```
Dell#mkdir nfsmount:/nfs-mountpoint/guest
```

Related Commands rmdir – removes a directory.

mount nfs

Mount an NFS file system to a device.

C9000 Series

Syntax `mount nfs rhost:path mount-point [username password]`

Parameters Enter the following location keywords and information:

rhost:path	Enter the remote hosts's path directory.

mount-point	Enter the folder name in the local file system.
username	(OPTIONAL) Enter the user name to access the device.
password	(OPTIONAL) Enter the password.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced this command.

Example

```
Dell#mount nfs nfstest nfs-mount-point usrname pwd
```

Related Commands cd – changes the working directory.

pwd

Display the current working directory.

C9000

Syntax `pwd`

From a **PE console**, use `pwd` to view the current working directory.

Defaults Crash kernel files are uploaded to flash by default.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

Example

```
Dell#pwd
flash:/default_diag_report_dir
```

Related Commands cd – changes the directory.

rename

Rename a file in the local file system.

C9000 Series

Syntax

`rename` *`url url`*

From a **PE console**, use `rename {flash:` *`directory name/path`* `|` `usbflash:` *`directory name/path`*`}`

Parameters

directory name/path — Enter the following keywords and a filename:

- For a file on the internal Flash, enter `flash://` and the filename.
- For a file on an NFS mounted file system, enter `nfsmount://` and the mount point and file path.
- For a file on an external USB drive, enter `usbflash://` and the filename.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added the `nfsmount:<mount-point>` parameters to support remote NFS file system.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on S-Series
7.5.1.0	Introduced on C-Series
E-Series	Original command

Usage Information

To rename a file in the local file system from a PE console, use the `rename {flash:` *`directory name/path`* `|` `usbflash` *`directory name/path`*`}` command .

restore factory-defaults

Restore factory defaults on a switch.

C9000 Series

Syntax

```
restore factory-defaults {chassis {bootvar | clear-all | nvram}| domain
{bootvar | clear-all | nvram} | linecard {slot-id | all} {bootvar| clear-all |
nvram} | pe {pe-id | all} {bootvar | clear-all | nvram}| rpm {slot-id | all}
{bootvar | clear-all | nvram}}
```

Parameters

chassis	Enter the keyword `chassis` to reset all the RPMs and line modules (LM).
domain	Enter the keyword `domain` to reset all the RPMs, LM, and port extenders (PE).
linecard *slot-id*	Enter the keyword `linecard` and the slot-id number. The *slot-id* range is from 0 to 11. Enter `linecard all` to reset all the linecards.
pe *pe-id*	Enter the keyword `pe` and the port extender (PE) ID. The *pe-id* range is from 0 to 255. Enter `pe all` to reset all the PEs.
rpm	Enter the keyword `rpm` to rest the RPM card.
bootvar	Enter the keyword `bootvar` to reset the boot environment variables only.
clear-all	Enter the keyword `clear-all` to reset the Bootvar, NvRam, and configurations.
nvram	Enter the keyword `nvram` to reset the NvRAM only.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.17.1	Supported on the M I/O Aggregator.

Usage Information

Restoring factory defaults deletes the existing startup configuration and all persistent settings (stacking, fanout, and so forth).

When restoring factory default settings, a switch remains in standalone mode after the restoration. After the restore is complete, the units power cycle immediately.

CAUTION: There is no undo for this command.

Example

```
Dell#restore factory-defaults chassis clear-all

    ********************************************************************
    *  Warning - Restoring factory defaults will delete the existing      *
    *  startup-config and resets all persistent settings (stacking,       *
    *  fanout, etc.) and boot environment variables (boot config, console *
    *  baud rate, management interface settings, etc.)                    *
    *  After restoration the unit(s) will be powercycled immediately.     *
    *  Proceed with caution !                                             *
    ********************************************************************
```

```
Proceed with factory settings? Confirm [yes/no]:
```

rmdir

Remove a directory from the NFS mounted file system.

C9000 Series

Syntax `rmdir nfsmount://mount-point/usrname`

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 Series.
9.7(0.0)	Introduced this command.

Example

```
Dell#rmdir nfsmount:/nfs-mountpoint/guest
Proceed to remove the directory [confirm yes/no]: yes
Dell#
```

Related Commands mkdir – creates a directory.

show boot bmp

Display the current state of bare metal provisioning (BMP) or the jump-start process.

C9000 Series

Syntax `show boot bmp`

Parameters

bmp	Display the current information on the state of BMP or the jump-start process.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Example

```
Dell#show boot bmp
Reload type is set to normal mode. BMP process is in disabled state
```

show boot system

Display information about boot images currently stored on the system.

C9000 Series

Syntax

```
show boot system all
```

From a **PE console**, use the following:

```
show boot system {stack-unit unit number | all}
```

Parameters

all	Display the boot images stored on the system for the Control Processor, Route Processor, and line card CPUs. From a PE console, display boot image information on all the unit.
stack-unit *unit-number*	Display the boot image information for a specified stack-unit. The stack-unit number range is from 0 to 7.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.

Example

```
Dell#show boot system all

Current system image information in the system:
===============================================

Type           Boot Type       A                    B
-----------------------------------------------------------
rpm 0 (CP)     DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
rpm 1 (CP)     DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
rpm 0 (RP)     DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
```

```
rpm 1 (RP)     DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
linecard 0     DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
linecard 1 is not present.
linecard 2     DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
linecard 3 is not present.
linecard 4 is not present.
linecard 5     DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
linecard 6     DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
linecard 7 is not present.
linecard 8 is not present.
inecard 9 is not present.
linecard 10    DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
linecard 11    DOWNLOAD BOOT   1-0(0-4074)          1-0(0-4081)
```

Example (PE Console)

```
Dell#show boot system stack-unit all

Current system image information in the system:
===============================================

Type           Boot Type       A                   B
-------------------------------------------------------------
stack-unit 0 is not present.
stack-unit 1   FLASH BOOT      1-0(0-3995)         1-0(0-4046)[boot]
stack-unit 2   FLASH BOOT      1-0(0-3995)         1-0(0-4046)[boot]
stack-unit 3   FLASH BOOT      1-0(0-3995)         1-0(0-4046)[boot]
stack-unit 4 is not present.
stack-unit 5 is not present.
stack-unit 6 is not present.
stack-unit 7 is not present.
```

show bootvar

Display the variable settings for the boot parameters.

C9000 Series

Syntax `show bootvar`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.4	Output expanded to display current reload mode (normal or Jumpstart).
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.

Version	Description
E-Series	Original command.

Example

```
Dell#show bootvar
PRIMARY IMAGE FILE =  ftp://ftp:ftp@10.11.227.233/tftpboot/FTOS-
VG-1-0-0-4079.bin
SECONDARY IMAGE FILE =  ftp://ftp:ftp@10.11.227.233/tftpboot/FTOS-
VG-1-0-0-4046.bin
DEFAULT IMAGE FILE =  system://A
LOCAL CONFIG FILE =  variable does not exist
PRIMARY HOST CONFIG FILE =  variable does not exist
SECONDARY HOST CONFIG FILE =  variable does not exist
PRIMARY NETWORK CONFIG FILE =  variable does not exist
SECONDARY NETWORK CONFIG FILE =  variable does not exist
CURRENT IMAGE FILE =  ftp://ftp:ftp@10.11.227.233/tftpboot/FTOS-
VG-1-0-0-4079.bin
CURRENT CONFIG FILE 1 =  flash://startup-config
CURRENT CONFIG FILE 2 =  variable does not exist
CONFIG LOAD PREFERENCE =  local first
BOOT INTERFACE GATEWAY IP ADDRESS =  10.11.93.254
Reload Mode =  normal-reload
```

Related Commands boot system — sets the location of Dell Networking OS image files.

show file

Display contents of a text file in the local filesystem.

C9000 Series

Syntax `show file` *`filesystem`*

From a **PE console**, use `show file` *`filesystem`* to view the contents of a text file.

Parameters

filesystem	Enter one of the following: • For internal flash, enter `flash:` • For USB flash, enter `usbflash:`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series
7.5.1.0	Introduced on the C-Series
E-Series	Original command

Example

```
Dell#show file flash://startup-config
! Version 1-0(0-4079)
! Last configuration change at Wed Jun 24 02:02:40 2015 by default
! Startup-config last updated at Wed Jun 24 02:02:44 2015 by default
!
boot system rpm0 primary tftp://10.11.227.233/pt-c9000-2
boot system rpm0 secondary system: A:
boot system rpm0 default system: A:
boot system rpm1 primary tftp://10.11.227.233/pt-c9000-2
boot system rpm1 secondary system: A:
boot system rpm1 default system: A:
!
service timestamps log datetime
!
logging coredump
!
hostname Dell
!
protocol lldp
!
feature extended-bridge
!
redundancy auto-failover-limit count 3 period 60
redundancy auto-synchronize full
!
redundancy disable-auto-reboot pe all
!
enable password 7 b125455cf679b208e79b910e85789edf
!
username admin password 7 1d28e9f33f99cf5c
!
linecard 0 provision C9000LC2410G
!
interface TenGigabitEthernet 0/0
!
protocol lldp
no shutdown
!
!
!
```

Example (PE Console)

Related Commands format flash — Erases all the existing files and reformats the file system in the internal flash memory.

show file-systems

Display information about the file systems on the system.

Syntax `show file-systems`

From a **PE console**, use `show file-systems` to view the file-system information.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series
7.5.1.0	Introduced on the C-Series
E-Series	Original command

Command Fields

Field	Description
size(b)	Lists the size (in bytes) of the storage location. If the location is remote, no size is listed.
Free(b)	Lists the available size (in bytes) of the storage location. If the location is remote, no size is listed.
Feature	Displays the formatted DOS version of the device.
Type	Displays the type of storage. If the location is remote, the word `network` is listed.
Flags	Displays the access available to the storage location. The following letters indicate the level of access: • r = read access • w = write access
Prefixes	Displays the name of the storage location.

Example

```
Dell#show file-systems
Size(b) Free(b) Feature Type Flags Prefixes
63938560 51646464 dosFs2.0 MMC rw flash:
63938560 18092032 dosFs1.0 MMC rw slot0:
- - - network rw ftp:
- - - network rw tftp:
- - - network rw scp:
Dell#
```

Example (PE Console)

```
Dell#show file-system

      Size(b)     Free(b)      Feature      Type   Flags  Prefixes
    100450304   100270080      Unknown USERFLASH      rw  flash:
            -           -  unformatted USERFLASH      rw  fcmfs:
            -           -  unformatted  NFSMOUNT      rw  nfsmount:
```

```
-           -           -    network      rw  ftp:
-           -           -    network      rw  tftp:
-           -           -    network      rw  scp:
-           -           -    network      rw  http:
-           -           -    network      rw  https:
```

show os-version

Display the release and software image version information of the image file specified.

C9000 Series

Syntax

`show os-version [file-url]`

From a **PE console**, use `show os-version` to view the release and software image information.

Parameters

file-url (OPTIONAL) Enter the following location keywords and information:

- For a file on the internal flash, enter `flash://` then the filename.
- For a file on an FTP server, enter `ftp://user:password@hostip/filepath.`
- For a file on an NFS-mounted system, enter `nfsmount://<mount-point/filepath>`

  NOTE: While switching to a remote NFS file system, it is mandatory to specify the mount-point that indicates the working directory on the NFS file system. You cannot enter the root directory of the remote NFS file system.
- For a file on a TFTP server, enter `tftp://hostip/filepath`.
- For a file on the USB port, enter `usbflash://filepath`.

NOTE: The port extender information is displayed only when the extended bridge feature is enabled.

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Usage Information

NOTE: A filepath that contains a dot (.) is not supported.

Example

```
Dell#show os-version

RELEASE IMAGE INFORMATION :
------------------------------------------------------------------------
      Platform          Version        Size           ReleaseTime
 C-Series:C9000         9.9(0.0)   125192571    Sep  8 2015 06:08:13

TARGET IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
       runtime         9.9(0.0)                      CP      passed
       runtime         9.9(0.0)                      LP      passed
       runtime         9.9(0.0)                      RP      passed
       runtime         9.9(0.0)                      cp      passed

BOOT IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
    boot flash         3.3.1.16                CP/RP/LP      passed

BOOTSEL IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
 boot selector          3.3.0.1                 CP/RP/LP      passed

FPGA IMAGE INFORMATION :
------------------------------------------------------------------------
         Card                        FPGA Name    Version
   linecard 0                            FPGA       3.10
   linecard 0                            CPLD        3.1
   linecard 0                             IAP        3.2
   linecard 1                            FPGA       3.10
   linecard 1                            CPLD        3.1
   linecard 1                             IAP        3.2
   linecard 2                            FPGA       3.10
   linecard 2                            CPLD        3.1
   linecard 2                             IAP        3.2
   linecard 3                            FPGA       3.10
   linecard 3                            CPLD        3.1
   linecard 3                             IAP        3.2
   linecard 4                            FPGA       3.10
   linecard 4                            CPLD        3.1
   linecard 4                             IAP        3.2
   linecard 5                            FPGA       3.10
   linecard 5                            CPLD        3.1
   linecard 5                             IAP        3.2
   linecard 6                            FPGA       3.10
   linecard 6                            CPLD        3.1
   linecard 6                             IAP        3.2
   linecard 7                            FPGA       3.10
   linecard 7                            CPLD        3.1
   linecard 7                             IAP        3.2
   linecard 8                            FPGA       3.10
   linecard 8                            CPLD        3.1
   linecard 8                             IAP        3.2
        RPM 0                         FPGA 1       3.12
        RPM 0                           CPLD        3.6
        RPM 0                         FPGA 2        2.0
        RPM 0                      Backup FPGA        2.0
```

```
        RPM 0                           IAP        3.2
        RPM 1                         FPGA 1       3.12
        RPM 1                           CPLD       3.6
        RPM 1                         FPGA 2       2.0
        RPM 1                   Backup FPGA        2.0
        RPM 1                           IAP        3.2
```

Example: PE

```
Dell#show os-version

RELEASE IMAGE INFORMATION :
------------------------------------------------------------------------
      Platform          Version        Size           ReleaseTime
 C-Series:C9000         9.9(0.0)   125192571    Sep  8 2015 06:08:13

TARGET IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
       runtime         9.9(0.0)                      CP      passed
       runtime         9.9(0.0)                      LP      passed
       runtime         9.9(0.0)                      RP      passed
       runtime         9.9(0.0)                      cp      passed

BOOT IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
    boot flash         3.3.1.16                CP/RP/LP      passed

BOOTSEL IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
 boot selector          3.3.0.1                 CP/RP/LP      passed

FPGA IMAGE INFORMATION :
------------------------------------------------------------------------
         Card                         FPGA Name    Version
   linecard 0                            FPGA       3.10
   linecard 0                            CPLD        3.1
   linecard 0                             IAP        3.2
   linecard 1                            FPGA       3.10
   linecard 1                            CPLD        3.1
   linecard 1                             IAP        3.2
   linecard 2                            FPGA       3.10
   linecard 2                            CPLD        3.1
   linecard 2                             IAP        3.2
   linecard 3                            FPGA       3.10
   linecard 3                            CPLD        3.1
   linecard 3                             IAP        3.2
   linecard 4                            FPGA       3.10
   linecard 4                            CPLD        3.1
   linecard 4                             IAP        3.2
   linecard 5                            FPGA       3.10
   linecard 5                            CPLD        3.1
   linecard 5                             IAP        3.2
   linecard 6                            FPGA       3.10
   linecard 6                            CPLD        3.1
   linecard 6                             IAP        3.2
   linecard 7                            FPGA       3.10
   linecard 7                            CPLD        3.1
   linecard 7                             IAP        3.2
   linecard 8                            FPGA       3.10
   linecard 8                            CPLD        3.1
   linecard 8                             IAP        3.2
        RPM 0                         FPGA 1       3.12
        RPM 0                           CPLD       3.6
        RPM 0                         FPGA 2       2.0
        RPM 0                   Backup FPGA        2.0
        RPM 0                           IAP        3.2
```

```
        RPM 1                          FPGA 1       3.12
        RPM 1                            CPLD        3.6
        RPM 1                          FPGA 2        2.0
        RPM 1                     Backup FPGA        2.0
        RPM 1                             IAP        3.2

PE RELEASE IMAGE INFORMATION :
------------------------------------------------------------------------
      Platform          Version        Size           ReleaseTime
 C-Series:C1048P         9.9(0.0)    27132884    Sep  8 2015 06:06:18

PE BOOT IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    Checksum
    boot flash          3.3.1.7        Control Processor      passed

PE FPGA IMAGE INFORMATION :
------------------------------------------------------------------------
     FPGA Name          Version
          CPLD               16

PE PoE-CONTROLLER IMAGE INFORMATION
------------------------------------------------------------------------
          Type          Version
PoE Controller              2.65
```

Example: PE Console

```
Dell#show os-version

RELEASE IMAGE INFORMATION :
------------------------------------------------------------------------
      Platform          Version        Size           ReleaseTime
 C-Series:C1048P         9.9(0.0)    27132884    Sep  8 2015 06:06:18

TARGET IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
       runtime         9.9(0.0)        Control Processor      passed

BOOT IMAGE INFORMATION :
------------------------------------------------------------------------
          Type          Version                   Target    checksum
    boot flash          3.3.1.7        Control Processor      passed

FPGA IMAGE INFORMATION :
------------------------------------------------------------------------
         Card                        FPGA Name    Version
 stack-unit 0                          CPLD         16
 stack-unit 1                          CPLD         16
```

show running-config

Display the current configuration and display changes from the default values.

C9000 Series

Syntax `show running-config [entity] [configured] [status]`

Parameters

entity	(OPTIONAL) To display that entity's current (non-default) configuration, enter one of the following keywords:

NOTE: If you did not configure anything that entity, nothing displays and the prompt returns.

aaa	for the current AAA configuration
acl	for the current ACL configuration
acl-vlan-group	for the current ACL VLAN Group configuration
arp	for the current static ARP configuration
as-path	for the current AS-path configuration
bfd	for the current BFD configuration
bgp	for the current BGP configuration
boot	for the current boot configuration
class-map	for the current class-map configuration
community-list	for the current community-list configuration
compressed	for the current operation configuration in compressed form
crypto	for the current crypto configuration
dcb-buffer-threshold	for the current Buffer Threshold configuration
dcb-map	for the current dcb-map configuration
ecmp-group	for the current ECMP group configuration
ethernet	for the current Ethernet CFM configuration
extcommunity-list	for the current extended community-list configuration
fcoe-map	for the current fcoe-map configuration
fefd	for the current FEFD configuration
frrp	for the current FRRP configuration
ftp	for the current FTP configuration
gvrp	for the current GVRP configuration
host	for the current host configuration
http	for the current HTTP configuration
igmp	for the current IGMP configuration
interface	for the current interface configuration
ip	for the current IP configuration
isis	for the current ISIS configuration
line	for the current line configuration
lldp	for the current LLDP configuration
logging	for the current logging configuration
mac	for the current MAC ACL configuration

mac-address-table	for the current MAC configuration
management-crypto	for the current Management port forwarding configuration
management-eis	for the current management EIS configuration
management-route	for the current Management port forwarding configuration
mld	for the current MLD configuration
monitor	for the current Monitor configuration
mroute	for the current Mroutes configuration
msdp	for the current MSDP configuration
ntp	for the current NTP configuration
openflow	for the current Openflow instances configuration
ospf	for the current OSPF configuration
pe	for the current Port Extender configuration
pim	for the current PIM configuration
policy-map-input	for the current input policy map configuration
policy-map-output	for the current output policy map configuration
po-failover-group	for the current port-channel failover-group configuration
prefix-list	for the current prefix-list configuration
privilege	for the current privilege configuration
qos	for the current qos configuration
qos-policy-input	for the current input QoS policy configuration
qos-policy-output	for the current output QoS policy configuration
radius	for the current RADIUS configuration
redirect-list	for the current redirect-list configuration
redundancy	for the current RPM redundancy configuration
reload-type	for the current reload-type configuration
resolve	for the current DNS configuration
rip	for the current RIP configuration
rmon	for the current RMON configuration
role	for the current role configuration
route-map	for the current route map configuration

screvt-handler	for the current Script Handler configuration
sflow	for the current sFlow configuration
snmp	for the current SNMP configuration
spanning-tree	for the current spanning tree configuration
static	for the current static route configuration
status	for the file status information
tacacs+	for the current TACACS+ configuration
tftp	for the current TFTP configuration
track	for the current object tracking configuration
udf-tcam	for the current UDF TCAM profiles configuration
uplink-state-group	for the uplink state group configuration
users	for the current users configuration
vlt	for the current VLT configuration
vrf	for the current VRF configuration
vxlan	for the current Vxlan instances configuration
wred-profile	for the current wred-profile configuration

configured	(OPTIONAL) Enter the keyword `configuration` to display line card interfaces with non-default configurations only.
status	(OPTIONAL) Enter the keyword `status` to display the checksum for the running configuration and the start-up configuration.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information The `status` option allows you to display the size and checksum of the running configuration and the startup configuration.

Example

```
Dell#show running-config
Current Configuration ...
! Version 9.2(1.0B2)
! Last configuration change at Thu Mar  6 02:10:35 2014 by default
!
boot system primary system: A:
boot system secondary system: A:
boot system default system: A:
boot system gateway 1.1.1.1
!...
```

Example

```
Dell#show running-config status
running-config checksum 0xB4B9BF03
startup-config checksum 0x8803620F
Dell#
```

show startup-config

Display the startup configuration.

C9000 Series

Syntax

```
show startup-config
```

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on S-Series
7.5.1.0	Introduced on the C-Series.

```
Dell#show startup-config
! Version 1-0(0-4074)
! Last configuration change at Mon Jun 22 07:48:07 2015 by admin
! Startup-config last updated at Mon Jun 22 12:40:26 2015 by default
!
boot system rpm0 primary system: A:
boot system rpm0 secondary ftp://ftp:ftp@10.11.227.233/tftpboot/FTOS-
VG-1-0-0-4046.bin
boot system rpm0 default system: A:
boot system rpm1 primary system: A:
boot system rpm1 secondary ftp://ftp:ftp@10.11.227.233/tftpboot/FTOS-
VG-1-0-0-4046.bin
boot system rpm1 default system: A:
```

```
boot system gateway 10.11.93.254
!
service timestamps log datetime
!
logging coredump
!
hostname Dell
! protocol lldp
!
feature extended-bridge
!
redundancy auto-failover-limit count 3 period 60
redundancy auto-synchronize full
redundancy disable-auto-reboot rpm
!
```

Related Commands show running-config – displays the current (running) configuration.

upgrade

Upgrade the bootflash, bootselector, or Dell Networking OS (system) image on the switch CPUs.

C9000 Series

Syntax

```
upgrade {bootflash—image | bootselector-image| system—image} [all | linecard [slot-id |all] [pe pe-id {stack-unit unit-number}] | rpm{0|1} {booted | flash: | ftp: | rpmA:| rpmB:| scp:| tftp: | usbflash:}
```

Parameters

bootflash-image	Enter the keyword `bootflash-image` to upgrade the bootflash image on the switch CPUs.
bootselector-image	Enter the keyword `bootselector-image` to upgrade the bootselector image on the switch CPUs. **Use this option only with TAC supervision.**
system-image	Enter the keyword `system-image` to upgrade the boot OS image stored in cache memory of the switch CPUs.
all	Enter the keyword `all` to upgrade the bootflash and bootselector images on the switch CPUs.
linecard *slot-id*	Enter the keyword `linecard` and specify the linecard *slot-id* . The linecard slot id range is from 0 to 11. Enter `linecard all` to select all linecards.
rpm *slot-id*	Enter the keyword `rpm` to upgrade Control and Route processors of the RPM . To upgrade standby RPM execute the command from primary RPM with `rpmA: | rpmB:`,option.
pe *pe-id*	Enter the keyword `pe` and specify the port extender ID number. The PE ID range is from 0 to 255. Enter `pe all` to upgrade all port extenders attached to the C9010.
stack-unit *unit-number*	Enter the keyword `stack-unit` and specify the stack unit number. The stack unit number range is from 0 to 7.
booted	Enter the keyword `booted` to upgrade C9000 CPUs using the currently loaded bootflash and bootselector image. This option is not applicable for the system image.

flash: | ftp: | tftpdud: | usbflash: *file-url*	Enter one of the file transfer methods and locations to specify where the software image (*file-url*), which you want to use to upgrade the currently loaded image, is stored: • `flash://filepath`. • `ftp://userid:password@host-ip/filepath` to upgrade from an FTP server, where *host-ip* is either an IPv4 dotted decimal address or an IPv6 [x:x:x:x::x] format address. • `tftp://host-ip/filepath` to upgrade from a TFTP server, where *host-ip* is either an IPv4 dotted decimal address or an IPv6 [x:x:x:x::x] format address. • `usbflash://filepath` to upgrade form an external flash device.
rpmA: | rpmB:	Specify the primary RPM's flash partition for upgrade.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Introduced on N20xx and N30xx series.
9.9 (0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0(0.0)	Added support for IPv6 for the `file-url` parameter.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000. Added support for the SSD on the Z9000 only.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added support for TFTP and SCP.
7.6.1.0	Introduced on the S-Series.

Usage Information A system message displays with status information about the bootflash upgrade.

RFC 3986 specifies that IPv6 host addresses in a uniform resource identifier (URI) must be enclosed in square brackets, [X:X:X:X::X]. For maximum flexibility, this command accepts IPv6 host addresses with or without the square brackets.

Reload the system after executing this command.

To upgrade the Dell Networking OS image on a port extender from an attached PE console, enter the `upgrade` command in EXEC mode.

In a dual homing setup, you can use this command only from the primary VLT peer.

Examples (upgrade bootflash-image all booted)

```
Dell#upgrade bootflash-image all booted

Current Boot information in the system:
==========================================

  Card          BootFlash    Current Version  New Version
```

```
--------------------------------------------------------------------
rpm 0 (CP)      Boot Flash   3.3.1.15        3.3.1.15
rpm 0 (RP)      Boot Flash   3.3.1.15        3.3.1.15
Linecard10      Boot Flash   3.3.1.15        3.3.1.15

 ********************************************************************
 *  Warning - Upgrading boot flash is inherently risky and should only *
 *  be attempted when necessary.  A failure at this upgrade may cause  *
 *  a board RMA.  Proceed with caution !                               *
 ********************************************************************

Proceed Boot Flash image for all cards [yes/no]: no
```

Example (upgrade bootselector-image all booted)

```
Dell#upgrade bootselector-image all booted

Current Boot information in the system:
=======================================

Card          BootSelector    Current Version New Version
--------------------------------------------------------------------
rpm 0 (CP)    Boot Selector   3.3.0.0c        3.3.0.0f
rpm 0 (RP)    Boot Selector   3.3.0.0c        3.3.0.0f
Linecard10    Boot Selector   3.3.0.0c        3.3.0.0f

********************************************************************
*  Warning - Upgrading boot selectors is inherently risky and should  *
*  only be attempted when necessary.  A failure at this upgrade may   *
*  cause a board RMA.  Proceed with caution !                         *
********************************************************************

Proceed Boot Selector image for all cards [yes/no]: no
```

upgrade system-image-os6

This command removes Dell Networking OS 9.x.x.x and installs Dell Networking OS 6.x.x.x on a N-series port extender, so that it can be used as a switch.

C9010

Syntax

```
upgrade system-image-os6 {pe {pe-id}} {stack-unit {stack-unit-id} {tftp:// | Scp:// | ftp:// | usbflash:// | flash://}
```

Parameters

NOTE: This command is a hidden command and would not show up in the Dell Networking OS help file. This command needs to be entered manually.

pe *pe-id*	Enter the keyword `pe` and specify the pe-id to sync the OS 6 image to the port extender.
stack-unit *stack-unit-id*	Enter the keyword `stack-unit` and specify the stack-unit ID which contains the port extender.
tftp://	Enter the location of the OS6 files on a tftp server.
Scp://	Enter the location of the OS6 files on a scp server.
ftp://	Enter the location of the OS6 files on a ftp server.
usbflash://	Enter the location of the OS6 files on a USB drive.
flash://	Enter the location of the OS6 files on a flash drive.

Default None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Introduced on the C9010

Usage Information If you previously installed Dell Networking OS 9.x.x.x on a N20xx or N30xx series device to use it as a port extender for a C9010, you can use the upgrade system-image-os6 command to install Dell Networking OS 6.x.x.x and use it as a switch.

verify

Validate the software image on the flash drive after the image has been transferred to the system, but before the image has been installed.

C9000 Series

Syntax `verify { md5 | sha256 }[ flash:// ] img-file [hash-value]`

Parameters

md5	Enter the `md5` keyword to use the MD5 message-digest algorithm.
sha256	Enter the `sha256` keyword to use the SHA256 Secure Hash Algorithm
flash://	(Optional). Enter the `flash://` keyword. The default is to use the flash drive. You can just enter the image file name.
img-file	Enter the name the Dell Networking software image file to validate.
hash-value	(Optional). Enter the relevant hash published on i-Support.

Default flash drive

Command Modes EXEC mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information You can enter this command in the following ways:

- **verify md5 flash**://*img-file*
- **verify md5 flash**://*img-file <hash-value>*
- **verify sha256 flash**://*img-file*

- **verify sha256 flash**://*img-file* <*hash-value*>

Example

Without Entering the Hash Value for Verification using SHA256

```
Dell# verify sha256 flash://FTOS-SE-9.5.0.0.bin
SHA256 hash for FTOS-SE-9.5.0.0.bin:
e6328c06faf814e6899ceead219afbf9360e986d692988023b749e6b2093e933
```

Entering the Hash Value for Verification using SHA256

```
Dell# verify sha256 flash://FTOS-SE-9.5.0.0.bin
e6328c06faf814e6899ceead219afbf9360e986d692988023b749e6b2093e933
SHA256 hash VERIFIED for FTOS-SE-9.5.0.0.bin
```

5

802.1X

An authentication server must authenticate a client connected to an 802.1X switch port. Until the authentication, only extensible authentication protocol over LAN (EAPOL) traffic is allowed through the port to which a client is connected. After authentication is successful, normal traffic passes through the port.

The Dell Networking OS supports remote authentication dial-in service (RADIUS) and active directory environments using 802.1X Port Authentication.

Important Points to Remember

The system limits network access for certain users by using virtual local area network (VLAN) assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- If the primary RADIUS server becomes unresponsive, the authenticator begins using a secondary RADIUS server, if configured.
- If no VLAN is supplied by the RADIUS server or if you disable 802.1X authorization, the port configures in its access VLAN after successful authentication.
- If you enable 802.1X authorization but the VLAN information from the RADIUS server is not valid, the port returns to the Unauthorized state and remains in the configured access VLAN. This safeguard prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If you enable 802.1X authorization and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If you enable port security on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If you disable 802.1X on the port, it returns to the configured access VLAN.
- When the port is in the Force Authorized, Force Unauthorized, or Shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.
- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

Topics:

- debug dot1x
- dot1x auth-fail-vlan
- dot1x auth-server
- dot1x auth-type mab-only
- dot1x authentication (Configuration)
- dot1x authentication (Interface)
- dot1x critical-vlan
- dot1x guest-vlan
- dot1x host-mode
- dot1x mac-auth-bypass
- dot1x max-eap-req
- dot1x max-supplicants
- dot1x port-control
- dot1x profile
- dot1x quiet-period

- dot1x reauthentication
- dot1x reauth-max
- dot1x server-timeout
- dot1x static-mab
- dot1x supplicant-timeout
- dot1x tx-period
- mac
- show dot1x cos-mapping interface
- show dot1x interface
- show dot1x profile

debug dot1x

Display 802.1X debugging information.

C9000 Series

Syntax `debug dot1x [all | auth-pae-fsm | backend-fsm | eapol-pdu] [interface interface]`

Parameters

all	Enable all 802.1X debug messages.
auth-pae-fsm	Enable authentication PAE FSM debug messages.
backend-fsm	Enable backend FSM debug messages.
eapol-pdu	Enable the EAPOL frame trace and related debug messages.
interface *interface*	Restricts the debugging information to an interface. The `interface` option is available only when the interface is either operationally up or dot1x related interface configuration exists before enabling debugging for that interface.

Defaults Disabled

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series and S-Series.

dot1x auth-fail-vlan

Configure an authentication failure VLAN for users and devices that fail 802.1X authentication.

C9000 Series

Syntax

`dot1x auth-fail-vlan` *`vlan-id`* `[max-attempts` *`number`*`]`

To delete the authentication failure VLAN, use the `no dot1x auth-fail-vlan` *`vlan-id`* `[max-attempts` *`number`*`]` command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is from 1 to 4094.
max-attempts *number*	(OPTIONAL) Enter the keywords `max-attempts` followed number of attempts desired before authentication fails. The range is from 1 to 5. The default is **3**.

Defaults

3 attempts

Command Modes

CONFIGURATION (*conf-if-interface-slot/port*)

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series and S-Series.

Usage Information

If the host responds to 802.1X with an incorrect login/password, the login fails. The switch attempts to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface moves to the authentication failed VLAN.

After the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication occurs at the next reauthentication interval (`dot1x reauthentication`).

Use this command in Configuration Terminal Batch mode to configure the authentication failure in a dual-homing setup.

Related Commands

- dot1x port-control
- dot1x guest-vlan
- show dot1x interface

dot1x auth-server

Configure the authentication server to RADIUS.

C9000 Series

Syntax `dot1x auth-server radius`

Defaults none

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x auth-type mab-only

To authenticate a device with MAC authentication bypass (MAB), only use the host MAC address.

C9000 Series

Syntax `dot1x auth-type mab-only`

Defaults Disabled

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Introduced on the C-Series and S-Series.

Usage Information The prerequisites for enabling MAB-only authentication on a port are:

- Enable 802.1X authentication globally on the switch and on the port (the `dot1x authentication` command).
- Enable MAC authentication bypass on the port (the `dot1x mac-auth-bypass` command).

In MAB-only authentication mode, a port authenticates using the host MAC address even though 802.1x authentication is enabled. If the MAB-only authentication fails, the host is placed in the guest VLAN (if configured).

To disable MAB-only authentication on a port, enter the `no dot1x auth-type mab-only` command.

Use this command in Interface Batch Mode to authenticate a device with MAB in a dual-homing setup.

Related Commands dot1x mac-auth-bypass

dot1x authentication (Configuration)

Enable dot1x globally. Enable dot1x both globally and at the interface level.

C9000 Series

Syntax `dot1x authentication`

To disable dot1x globally, use the `no dot1x authentication` command.

Defaults Disabled

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

Related Commands dot1x authentication (Interface)

dot1x authentication (Interface)

Enable dot1x on an interface. Enable dot1x both globally and at the interface level.

C9000 Series

Syntax `dot1x authentication`

To disable dot1x on an interface, use the `no dot1x authentication` command.

Defaults Disabled

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information Use this command to enable dot1x on an interface. Use in the Interface Batch Mode to enable dot1x on an interface in a dual-homing setup.

Related Commands dot1x authentication (Configuration)

dot1x critical-vlan

Configure critical-VLAN for users or devices when authentication server is not reachable.

Syntax `[no] dot1x critical-vlan vlan-id`

Parameters

vlan-id	Enter the VLAN identifier. The VLAN-ID range is from 1 to 4094.

Defaults Not Configured.

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the S3100 series, S4048–ON, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, the Configuration Terminal Batch mode on C9010, Z9100–ON, and Z9500.
9.9(0.0)	Introduced on the C9000 Series.

Usage Information The `dot1x critical-vlan` command configures critical VLAN for the interface. If the authentication server is not reachable or not responding, the authenticator places the port or the supplicant in critical VLAN within the first attempt.

Use this command in Interface Batch mode to configure critical VLAN for users in a dual-homing setup.

Example

```
Dell(conf)#show dot1x interface ten gigabit ethernet 0/41

802.1x information on Te 0/41:
------------------------------
Dot1x Status:                  Enable
Port Control:                  AUTO
Port Auth Status:              AUTHORIZED (CRITICAL-VLAN)
Re-Authentication:             Enable
Untagged VLAN id:              400
Guest VLAN:                    Enable
```

```
Guest VLAN id:              400
Auth-Fail VLAN:             Enable
Auth-Fail VLAN id:          400
Auth-Fail Max-Attempts:     3
Critical VLAN:              Enable
Critical VLAN id:           400
Mac-Auth-Bypass:            Disable
Mac-Auth-Bypass Only:       Disable
Tx Period:                  30 seconds
Quiet Period:               60 seconds
ReAuth Max:                 2
Supplicant Timeout:         30 seconds
Server Timeout:             30 seconds
Re-Auth Interval:           60 seconds
Max-EAP-Req:                2
Host Mode:                  SINGLE_HOST
Auth PAE State:             Authenticated
Backend State:              Idle
```

dot1x guest-vlan

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

C9000 Series

Syntax

`dot1x guest-vlan` *vlan-id*

To disable the guest VLAN, use the `no dot1x guest-vlan` *vlan-id* command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION (*conf-if-interface-slot/port*)

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series, E-Series, and S-Series.

Usage Information

802.1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN.

If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface and authentication, for the device, occurs at the next reauthentication interval (`dot1x reauthentication`).

If the host fails authentication for the designated number of times, the authenticator places the port in authentication failed VLAN (`dot1x auth-fail-vlan`).

NOTE: You can create the Layer 3 portion of a guest VLAN and authentication fail VLANs regardless if the VLAN is assigned to an interface or not. After an interface is assigned a guest VLAN (which has an IP address), routing through the guest VLAN is the same as any other traffic. However, the interface may join/leave a VLAN dynamically.

Use this command in Configuration Terminal Batch mode to configure a guest VLAN in a dual-homing setup.

Related Commands

- dot1x auth-fail-vlan
- dot1x reauthentication
- dot1x reauth-max
- show dot1x interface

dot1x host-mode

Enable single-host or multi-host authentication.

C9000 Series

Syntax

```
dot1x host-mode {single-host | multi-host | multi-auth}
```

Parameters

single-host	Enable single-host authentication.
multi-host	Enable multi-host authentication.
multi-auth	Enable multi-supplicant authentication.

Defaults

single-host

Command Modes

INTERFACE

INTERFACE (BATCH MODE)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Added the `multi-auth` option on the C-Series and S-Series.
8.3.2.0	Added the `single-host` and `multi-host` options on the C-Series, E-Series, and S-Series.

Usage Information

- Single-host mode authenticates only one host per authenticator port and drops all other traffic on the port.
- Multi-host mode authenticates the first host to respond to an Identity Request and then permits all other traffic on the port.
- Multi-supplicant mode authenticates every device attempting to connect to the network on the authenticator port.
- Use this command in Interface Batch Mode to enable single-host or multi-host authentication in a dual-homing setup.

Related Commands show dot1x interface

dot1x mac-auth-bypass

Enable MAC authentication bypass. If 802.1X times out because the host did not respond to the Identity Request frame, the system attempts to authenticate the host based on its MAC address.

C9000 Series

Syntax `dot1x mac-auth-bypass`

To disable MAC authentication bypass on a port, use the `no dot1x mac-auth-bypass` command.

Defaults Disabled

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series and S-Series.

Related Commands dot1x auth-type mab-only

dot1x max-eap-req

Configure the maximum number of times an extensive authentication protocol (EAP) request is transmitted before the session times out.

C9000 Series

Syntax `dot1x max-eap-req number`

To return to the default, use the `no dot1x max-eap-req` command.

Parameters

number	Enter the number of times an EAP request is transmitted before a session time-out. The range is from 1 to 10. The default is **2**.

Defaults **2**

Command Modes INTERFACE

ITNERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x max-supplicants

Restrict the number of supplicants that can be authenticated and permitted to access the network through the port. This configuration is only takes effect in Multi-Auth mode.

C9000 Series

Syntax `dot1x max-supplicants number`

Parameters

number	Enter the number of supplicants that can be authenticated on a single port in Multi-Auth mode. The range is from 1 to 128. The default is **128**.

Defaults 128 hosts can be authenticated on a single authenticator port.

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the C-Series and S-Series.

Related Commands dot1x host-mode

dot1x port-control

Enable port control on an interface.

C9000 Series

Syntax `dot1x port-control {force-authorized | auto | force-unauthorized}`

Parameters

force-authorized	Enter the keywords `force-authorized` to forcibly authorize a port.

	auto	Enter the keyword `auto` to authorize a port based on the 802.1X operation result.
	force-unauthorized	Enter the keywords `force-unauthorized` to forcibly deauthorize a port.

Defaults none

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information The authenticator completes authentication only when `port-control` is set to `auto`.

Use this command in Interface Batch Mode to enable port control on an interface in a dual-homing setup.

dot1x profile

Configure a dot1x profile to define a list of trusted supplicant MAC addresses.

Syntax `[no] dot1x profile` *`profile-name`*

Parameters

	profile-name	Enter a dot1x *`profile-name`*. The profile name length is limited to 32 characters.

Defaults None

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Error Strings NONE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the S3100 series, S4048–ON, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, the Configuration Terminal Batch mode on C9010, Z9100–ON, and Z9500.
9.9(0.0)	Introduced on the C9010.

Usage Information

The `dot1x profile` command configures a dot1x profile to define a list of trusted supplicant MAC addresses. Maximum number of dot1x profiles is limited to 10. This command launches dot1x profile mode for entering profile related commands such as the `mac` command. The `dot1x static-mab` command assigns the dot1x profile to an interface.

Use this command in Configuration Terminal Batch mode to configure the dot1x profile in a dual-homing setup.

Related Commands

- dot1x static-mab
- mac

dot1x quiet-period

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

C9000 Series

Syntax

`dot1x quiet-period` *seconds*

To disable quiet time, use the `no dot1x quiet-time` command.

Parameters

seconds	Enter the number of seconds. The range is from 1 to 65535. The default is **60**.

Defaults

60 seconds

Command Modes

INTERFACE

INTERFACE (BATCH MODE)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Version	Description
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x reauthentication

Enable periodic reauthentication of the client.

C9000 Series

Syntax

`dot1x reauthentication [interval seconds]`

To disable periodic reauthentication, use the `no dot1x reauthentication` command.

Parameters

interval *seconds*	(Optional) Enter the keyword `interval` then the interval time, in seconds, after which reauthentication is initiated. The range is from 1 to 31536000 (one year). The default is **3600** (1 hour).

Defaults

3600 seconds (1 hour)

Command Modes

INTERFACE

INTERFACE (BATCH MODE)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x reauth-max

Configure the maximum number of times a port can reauthenticate before the port becomes unauthorized.

C9000 Series

Syntax `dot1x reauth-max number`

To return to the default, use the `no dot1x reauth-max` command.

Parameters

number	Enter the permitted number of reauthentications. The range is from 1 to 10. The default is **2**.

Defaults **2**

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x server-timeout

Configure the amount of time after which exchanges with the server time-out.

C9000 Series

Syntax `dot1x server-timeout seconds`

To return to the default, use the `no dot1x server-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults **30** seconds

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information When you configure the `dot1x server-timeout` value, take into account the communication medium used to communicate with an authentication server and the number of RADIUS servers configured. Ideally, the `dot1x server-timeout` value (in seconds) is based on the configured RADIUS-server timeout and retransmit values and calculated according to the following formula: `dot1x server-timeout` *seconds* > (radius-server retransmit *seconds* + 1) * radius-server timeout *seconds*.

Where the default values are as follows: `dot1x server-timeout` (30 seconds), radius-server retransmit (3 seconds), and radius-server timeout (5 seconds).

For example:

```
Dell(conf)#radius-server host 10.11.197.105 timeout 6
Dell(conf)#radius-server host 10.11.197.105 retransmit 4
Dell(conf)#interface tengigabitethernet 2/23
Dell(conf-if-te-2/23)#dot1x server-timeout 40
```

Use this command in Interface Batch Mode to configure the server time-out in a dual-homing setup.

dot1x static-mab

Enable static MAC authorization bypass (MAB) and configure static MAB profile to an interface.

Syntax

```
[no] dot1x static-mab profile profile-name
```

Parameters

profile *profile-name*	Enter the keyword `profile` and the *profile-name* to configure the static MAB profile name. The profile name length is limited to 32 characters.

Defaults

Disabled.

Command Modes

INTERFACE

INTERFACE (BATCH MODE)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the S3100 series, S4048–ON, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, the Configuration Terminal Batch mode on C9010, Z9100–ON, and Z9500.
9.9(0.0)	Introduced on the C9010.

Usage Information

The `dot1x static-mab` command enables static MAB (mac auth bypass) and configures the associated profile on a dot1x interface. Static MAB bypasses the authentication server for the supplicant MAC addresses configured in the associated profile.

Before you enable static MAB, you must do the following:

- Enable MAC authentication bypass on the port by configuring the `dot1x mac-auth-bypass` command.
- Ensure that no configured profile exists at the time of configuring the `static-mab` command.
- Use this command in Interface Batch Mode to enable static MAB in a dual-homing setup.

Example

```
Dell(conf)#do show dot1x interface ten gigabit ethernet 0/41
802.1x information on Te 0/41:
---------------------------------------
Dot1x Status:              Enable
Port Control:              AUTO
Port Auth Status:          AUTHORIZED (STATIC-MAB)
Re-Authentication:         Enable
Untagged VLAN id:          400
Guest VLAN:                Enable
Guest VLAN id:             400
Auth-Fail VLAN:            Enable
Auth-Fail VLAN id:         400
Auth-Fail Max-Attempts:    3
Critical VLAN:             Enable
Critical VLAN id:          400
Mac-Auth-Bypass:           Disable
Mac-Auth-Bypass Only:      Disable
Static-MAB:                Enable
Static-MAB Profile:        Sample
Tx Period:                 30 seconds
Quiet Period:              60 seconds
```

```
ReAuth Max:               2
Supplicant Timeout:       30 seconds
Server Timeout:           30 seconds
Re-Auth Interval:         60 seconds
Max-EAP-Req:              2
Host Mode:                SINGLE_HOST
Auth PAE State:           Authenticated
Backend State:            Idle
```

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time-out.

C9000 Series

Syntax

`dot1x supplicant-timeout` *seconds*

To return to the default, use the `no dot1x supplicant-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults

30 seconds

Command Modes

INTERFACE

INTERFACE (BATCH MODE)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x tx-period

Configure the intervals at which EAPOL PDUs the Authenticator PAE transmits.

C9000 Series

Syntax `dot1x tx-period seconds`

To return to the default, use the `no dot1x tx-period` command.

Parameters

seconds	Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is from 1 to 65535. The default is **30**.

Defaults **30** seconds

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

mac

Configure a list of supplicant MAC addresses for dot1x profile represented with a profile-name.

Syntax `[no] mac {mac-address1 mac-address2… mac-address6}`

Parameters

mac-address1 mac-address2… mac-address6	Enter the keyword `mac` and type the 48– bit MAC addresses using the H.H.H format. A maximum of 6 MAC addresses are allowed.

Defaults None

Command Modes DOT1X PROFILE CONFIG (conf-dot1x-profile)

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the S3100 series, S4048–ON, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, the Configuration Terminal Batch mode on C9010, Z9100–ON, and Z9500.
9.9(0.0)	Introduced on the C9010.

Usage Information The `mac` command configures a list of supplicant MAC addresses for a dot1x profile represented with a profile-name. You can configure up to 6 MAC addresses in a single `mac` command. The maximum number of MAC addresses that you can configure in a single profile is limited to 100.

Use this command in Configuration Terminal Batch mode to configure a list of supplicant MAC addresses for dot1x profile in a dual-homing setup.

Example

```
Dell(conf)#dot1x profile mySupplicants
Dell(conf-dot1x-profile)#mac 00:50:56:AA:01:10 00:50:56:AA:01:11

Dell(conf-dot1x-profile)#show config
dot1x profile mySupplicants
 mac 00:50:56:aa:01:10
 mac 00:50:56:aa:01:11
Dell(conf-dot1x-profile)#
Dell(conf-dot1x-profile)#exit
```

show dot1x cos-mapping interface

Display the CoS priority-mapping table the RADIUS server provides and applies to authenticated supplicants on an 802.1X-enabled system.

C9000 Series

Syntax `show dot1x cos-mapping interface` *`interface`* `[mac-address` *`mac-address`*`]`

Parameters

interface Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

mac-address (Optional) MAC address of an 802.1X-authenticated supplicant.

Defaults none

Command Modes

- EXEC
- EXEC privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Introduced on the C-Series and S-Series.

Usage Information Enter a supplicant's MAC address using the `mac-address` option to display CoS mapping information only for the specified supplicant.

You can display the CoS mapping information applied to traffic from authenticated supplicants on 802.1X-enabled ports that are in Single-Hot, Multi-Host, and Multi-Supplicant authentication modes.

Example

```
Dell#show dot1x cos-mapping interface gigabitethernet 2/21

802.1p CoS re-map table on Gi 2/21:
-----------------------------------
Dot1p   Remapped Dot1p
0       7
1       6
2       5
3       4
4       3
5       2
6       1
7       0

Dell#show dot1x cos-mapping int g 2/21 mac-address 00:00:01:00:07:00

802.1p CoS re-map table on Gi 2/21:
-----------------------------------

802.1p CoS re-map table for Supplicant: 00:00:01:00:07:00
Dot1    Remapped Dot1p
0       7
1       6
2       5
3       4
4       3
5       2
6       1
7       0
```

show dot1x interface

Display the 802.1X configuration of an interface.

C9000 Series

Syntax

```
show dot1x interface interface [mac-address mac-address]
```

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
mac-address	(Optional) MAC address of a supplicant.

Defaults

none

Command Modes

- EXEC
- EXEC privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Added the `mac-address` option on the C-Series and S-Series.
7.6.1.0	Introduced on the C-Series, E-Series, and S-Series.

Usage Information

If you enable 802.1X multi-supplicant authentication on a port, additional 802.1X configuration details (Port Authentication status, Untagged VLAN ID, Authentication PAE state, and Backend state) are displayed for each supplicant, as shown in the following example.

Example

```
Dell#show dot1x int tengig 2/32

802.1x information on Te 2/32:
-----------------------------
Dot1x Status:           Enable
Port Control:           AUTO
Port Auth Status:       UNAUTHORIZED
```

```
Re-Authentication:      Disable
Untagged VLAN id:       None
Guest VLAN:             Enable
Guest VLAN id:          10
Auth-Fail VLAN:         Enable
Auth-Fail VLAN id:      11
Auth-Fail Max-Attempts: 3
Tx Period:              30 seconds
Quiet Period:           60 seconds
ReAuth Max:             2
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       3600 seconds
Max-EAP-Req:            2
Auth Type:              SINGLE_HOST
Auth PAE State:         Initialize
Backend State:          Initialize
Dell#
```

Example (mac-address)

```
Dell#show dot1x interface tengig 2/21 mac-address 00:00:01:00:07:00

802.1x information on Te 2/21:
------------------------------
Dot1x Status:           Enable
Port Control:           AUTO
Re-Authentication:      Disable
Guest VLAN:             Disable
Guest VLAN id:          NONE
Auth-Fail VLAN:         Disable
Auth-Fail VLAN id:      NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass:        Enable
Mac-Auth-Bypass Only:   Disable
Tx Period:              5 seconds
Quiet Period:           60 seconds
ReAuth Max:             1
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       60 seconds
Max-EAP-Req:            2
Host Mode:              MULTI_AUTH
Max-Supplicants:        128

Port status and State info for Supplicant: 00:00:01:00:07:00

Port Auth Status:       AUTHORIZED(MAC-AUTH-BYPASS)
Untagged VLAN id:       4094
Auth PAE State:         Authenticated
Backend State:          Idle
Dell#
```

Example (Interface)

```
Dell#show dot1x interface tengig 0/21

802.1x information on Te 0/21:
------------------------------
Dot1x Status:           Enable
Port Control:           AUTO
Re-Authentication:      Disable
Guest VLAN:             Enable
Guest VLAN id:          100
Auth-Fail VLAN:         Disable
Auth-Fail VLAN id:      NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass:        Disable
Mac-Auth-Bypass Only:   Disable
Tx Period:              30 seconds
Quiet Period:           60 seconds
ReAuth Max:             3
```

```
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       60 seconds
Max-EAP-Req:            2
Host Mode:              MULTI_AUTH
Max-Supplicants:        128

Port status and State info for Supplicant: 00:00:00:00:00:10

Port Auth Status:       AUTHORIZED
Untagged VLAN id:       400
Auth PAE State:         Authenticated
Backend State:          Idle

Port status and State info for Supplicant: 00:00:00:00:00:11
192 | 802.1X
www.dell.com | s u p p o r t . d e l l.com
Port Auth Status:       AUTHORIZED
Untagged VLAN id:       300
Auth PAE State:         Authenticated
Backend State:          Idle

Port status and State info for Supplicant: 00:00:00:00:00:15

Port Auth Status:       AUTHORIZED(GUEST-VLAN)
Untagged VLAN id:       100
Auth PAE State:         Authenticated
Backend State:          Idle
```

show dot1x profile

Display all the dot1x profiles or the details of a specific profile configured in the system.

C9000 Series

Syntax `show dot1x profile profile-name`

Parameters

profile-name	Specify a static dot1x *profile-name*. The maximum character limit for a profile name is 32 characters.

Defaults None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Example

```
Dell#show dot1x profile

802.1x profile information
------------------------------
Dot1x Profile mySupplicants
```

```
Profile MACs
 00:50:56:aa:01:10 00:50:56:aa:01:11
```

6

Access Control Lists (ACL)

Access control lists (ACLs) are supported on the Dell Networking operating system on the switch.
The following types of ACL, IP prefix list, and route maps are supported:

- Commands Common to all ACL Types
- Common IP ACL Commands
- Standard IP ACL Commands
- Extended IP ACL Commands
- Standard MAC ACL Commands
- Extended MAC ACL Commands
- IP Prefix List Commands
- Route Map Commands
- AS-Path Commands
- IP Community List Commands

NOTE: The number of entries allowed in an ACL is hardware-dependent. For information on the commands to use to re-allocate and display CAM memory space on the switch for Layer 2, IPv4, and IPv6 ACLs, refer to the Content Addressable Memory (CAM) chapter.

NOTE: For ACL commands that use the Trace function, refer to the Trace List Commands section in the Security chapter.

NOTE: For IPv6 ACL commands, refer to IPv6 Access Control Lists (IPv6 ACLs).

Topics:

- Commands Common to all ACL Types
- Common IP ACL Commands
- Standard IP ACL Commands
- Extended IP ACL Commands
- ACL VLAN Group Commands
- Common MAC ACL Commands
- Standard MAC ACL Commands
- Extended MAC ACL Commands
- IP Prefix List Commands
- Route Map Commands
- AS-Path Commands
- IP Community List Commands

Commands Common to all ACL Types

The following commands are available within each ACL mode and do not have mode-specific options. Some commands in this chapter may use similar names, but require different options to support the different ACL types (for example, the `deny` and `permit` commands).

remark

Enter a description for an ACL entry.

Syntax

`remark remark-number description`

To remove a remark, use the `no remark` command.

Parameters

remark-number	(Optional) Enter the remark number. The range is from 0 to 65535 for MAC ACL and 0 to 4294967290 for IP ACL. **NOTE: You can use the same sequence number for the remark and an ACL rule.**
description	Enter a description of up to 80 characters.

Defaults

Not configured.

Command Modes

- CONFIGURATION-STANDARD-ACCESS-LIST
- CONFIGURATION-EXTENDED-ACCESS-LIST
- CONFIGURATION-MAC ACCESS LIST-STANDARD
- CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14.0.0	Made the remark number as an optional value.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000–ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.4.1.0	Introduced on the E-Series.

Usage Information

The `remark` command is available in each ACL mode. You can configure up to 4294967291 remarks for a given IP ACL and 65536 remarks for a given MAC ACL.

You can include a remark with or without a remark number. If you do not enter a remark number, the remark inherits the sequence number of the last ACL rule. If there is no ACL rule when you enter a remark, the remark takes sequence number 5. If you configure two remarks with the same sequence number and different strings, the second one replaces the first string. You cannot configure two or more remarks with the same string and different sequence numbers.

To remove a remark, use the `no remark` command with or without the sequence number. If there is a matching string, the system deletes the remark.

Example

The following example shows the use of the `remark` command twice within CONFIGURATION-STANDARD-ACCESS-LIST mode. The remark precedes the rule in the running configuration because it is assumed that the remark is for the rule with the same sequence number, or the group of rules that follow the remark.

```
DellEMC(config-std-nacl)# remark 10 Deny rest of the traffic
DellEMC(config-std-nacl)# remark 5 Permit traffic from XYZ Inc.
DellEMC(config-std-nacl)# show config
!
ip access-list standard test
remark 5 Permit traffic from XYZ Inc.
seq 5 permit 1.1.1.0/24
remark 10 Deny rest of the traffic
seq 10 deny any
DellEMC(config-std-nacl)#
```

The following example shows adding a remark without a sequence number:

```
DELLEMC(config-ext-nacl)#permit ip any any
DELLEMC(config-ext-nacl)#remark permit any ip
DELLEMC(config-ext-nacl)#show c
!
ip access-list extended testac
 seq 5 permit ip any any
 remark 5 permit any ip
```

The following example shows that the system displays an error message when the same remark string is used with different remark numbers.

```
DELLEMC(config-ext-nacl)#seq 100 permit ip any any
DELLEMC(config-ext-nacl)#remark 10 permit any ip
DELLEMC(config-ext-nacl)#remark permit any ip
DELLEMC(config-ext-nacl)#% Error : Remark string already exists
```

Related Commands

- show config — display the current ACL configuration.

show config

Display the current ACL configuration.

C9000 Series

Syntax

```
show config
```

Command Modes

- CONFIGURATION-IP ACCESS LIST-STANDARD
- CONFIGURATION-IP ACCESS LIST-EXTENDED
- CONFIGURATION-MAC ACCESS LIST-STANDARD
- CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(config-ext-nacl)#show conf
!
ip access-list extended patches
Dell(config-ext-nacl)#
```

Common IP ACL Commands

The following commands are available within both IP ACL modes (Standard and Extended) and do not have mode-specific options. When an ACL is created without a rule and then is applied to an interface, ACL behavior reflects an implicit permit.

The C9000 supports both Ingress and Egress IP ACLs.

NOTE: Also refer to the Commands Common to all ACL Types section.

clear counters ip access-group

Erase all counters maintained for access lists.

C9000 Series

Syntax `clear counters ip access-group [access-list-name]`

Parameters

access-list-name	(OPTIONAL) Enter the name of a configured access-list, up to 140 characters.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increase the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

ip access-group

Assign an IP access list (IP ACL) to an interface.

Syntax `ip access-group access-list-name {in | out} [implicit-permit] [vlan vlan-id] [vrf vrf-name]`

To delete an IP access-group configuration, use the `no ip access-group access-list-name {in | out} [implicit-permit] [vlan vlan-id][layer3]` command.

Parameters

access-list-name	Enter the name of a configured access list, up to 140 characters.
in	Enter the keyword `in` to apply the ACL to incoming traffic.
out	Enter the keyword `out` to apply the ACL to outgoing traffic.

implicit-permit	(OPTIONAL) Enter the keyword `implicit-permit` to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the ID numbers of the VLANs. The range is from 1 to 4094 (you can use IDs from 1 to 4094).
vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` then the ID numbers of the VRFs. The range is from 1 to 63 (you can use IDs from 1 to 63). **NOTE: When you specify a single VRF, use the name of the VRF instead of the VRF ID number. Use the VRF ID numbers only when you specify a range of VRFs.**
layer3	(OPTIONAL) Enter the keyword `layer3` to enable layer 3 mode. It ensures that all the ACL rules in the access-group are applied only for L3 router packets.

Defaults Not enabled.

Command Modes INTERFACE/VRF MODE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000–ON.
9.4.(0.0)	Added support for VRF.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information You can assign one ingress ACL and one egress ACL to an interface.

NOTE: This command supports Loopback interfaces EE3 and EF series route processor modules (RPMs). This command does not support Loopback interfaces ED series RPMs and S-Series Loopback interfaces.

NOTE: If you apply outbound(egress) IP acl on a switch port, the filter applies only for routed traffic egressing out of that port.

To associate an access-list to a non-default VRF, use the `vrf` attribute of this command. You can use this command at the interface context (physical/LAG) to apply the access-list to a range of VRFs.

The VRF MODE is not available for the default and management VRFs.

In the Dell EMC Networking OS versions prior to 9.13(0.0), the system does not install any of your ACL rules if the available CAM space is lesser than what is required for your set of ACL rules. Effective with the Dell EMC Networking OS version 9.13(0.0), the system installs your ACL rules until all the allocated CAM memory is used. If there is no implicit permit in your rule, the Dell EMC Networking OS ensures that an implicit deny is installed at the end of your rule. This behavior is applicable for IPv4 and IPv6 ingress and egress ACLs.

One of the usage scenarios for using the **layer3** keyword at the VLAN level, is to avoid ACL being applied on the L2 traffic which comes in via ICL.

NOTE: The usage scenario listed above is one of many other usage scenarios.

Related Commands

- ip access-list standard — configure a standard ACL.
- ip access-list extended — configure an extended ACL.

ip control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv4 CPU traffic.

C9000 Series

Syntax

```
ip control-plane egress-filter
```

Defaults

Not enabled.

Command Modes

EXEC Privilege

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

show ip accounting access-list

Display the IP access-lists created on the switch and the sequence of filters.

C9000 Series

Syntax

```
show ip accounting {access-list access-list-name | cam_count} interface interface
```

Parameters

access-list-name	Enter the name of the ACL to be displayed.
cam_count	List the count of the CAM rules for this ACL.
interface *interface*	Enter the keyword `interface` then the one of the following keywords and slot/port or number information: • For a Port Channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
in | out	Identify whether ACL is applied on the ingress or egress side.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for the 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced.

Usage Information

show ip accounting access-lists Field	Description
"Extended IP..."	Displays the name of the IP ACL.
"seq 5..."	Displays the filter. If the keywords `count` or `byte` were configured in the filter, the number of packets or bytes the filter processes is displayed at the end of the line.
"order 4"	Displays the QoS order of priority for the ACL entry.

Example

```
Dell#show ip accounting access FILTER1 interface tengig 1/6
Extended IP access list FILTER1
seq 5 deny ip any 191.1.0.0 /16 count (0x00 packets)
seq 10 deny ip any 191.2.0.0 /16 order 4
seq 15 deny ip any 191.3.0.0 /16
seq 20 deny ip any 191.4.0.0 /16
seq 25 deny ip any 191.5.0.0 /16
```

Standard IP ACL Commands

When you create an ACL without any rule and then apply it to an interface, the ACL behavior reflects an implicit permit.

The C9000 supports both Ingress and Egress IP ACLs.

NOTE: Also refer to the Commands Common to all ACL Types and Common IP ACL Commands sections.

deny

Configure a filter that drops IP packets meeting the filter criteria.

C9000 Series

Syntax

`deny {`*`source mask`*` | any | host `*`ip-address`*`} [count [byte] | [dscp `*`value`*`] [order] [fragments] [log [interval `*`minutes`*`] [threshold-in-msgs [`*`count`*`]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq `*`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny {`*`source`*` [`*`mask`*`] | any | host `*`ip-address`*`}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.

any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
count	(OPTIONAL) Enter the keyword `count` to count packets that the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes that the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the `monitor` option.

Version	Description
6.5.1.0	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *C9000 Series Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

The software cannot count both packets and bytes, so when you enter the count byte options, only bytes are incremented.

Related Commands

ip access-list standard — configures a standard ACL.

permit — configures a permit filter.

feature acloptimized

Enable the acloptimized feature, and optimize ACL to increase the number of the IPv4 ACL rules.

Syntax

```
feature acloptimized
```

To remove this feature and bring the system to default, use the `no feature acloptimized` command, save the configuration, and reload the system.

Defaults

Not configured.

Command Modes

CONFIGURATION mode

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13(0.0)	Introduced on the S6100–ON and Z9100–ON.

Usage Information

After enabling the acloptimized feature, reboot the system.

Example

```
DellEMC(conf)#feature acloptimized
Configuration change will be in effect after save and reload. ACL config
containing TTL, layer3 and VRF conflicts with ACL Cam optimzation feature and
these keywords would be discarded while applying the ACL.
```

ip access-list standard

Create a standard IP access list (IP ACL) to filter based on IP address.

C9000 Series

Syntax

`ip access-list standard` *`access-list-name`*

To delete an access list, use the `no ip access-list standard` *`access-list-name`* command.

Parameters

access-list-name	Enter a string up to 140 characters long as the ACL name.

Defaults

All IP access lists contain an implicit "deny any"; that is, if no match occurs, the packet is dropped. ACL permit/deny rules are applied when a packet matches the condition in an entry.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to version 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the `monitor` option.
6.5.1.0	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

The system supports one ingress and one egress IP ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed information on the number entries allowed per ACL on the C9000, refer to the Content Addressable Memory (CAM) chapter in the *C9000 Configuration Guide*.

Use this command in Configuration Terminal Batch mode to create a standard IP access list in a dual-homing setup.

Example

```
Dell(conf)#ip access-list standard TestList
Dell(config-std-nacl)#
```

Related Commands

ip access-list extended — creates an extended access list.

show config — displays the current configuration.

permit

Configure a filter to permit packets from a specific source IP address to be processed and forwarded to another interface on the switch.

C9000 Series

Syntax

`permit {source [mask]| any | host ip-address}[count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {source [mask] | any | host ip-address}` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
count	(OPTIONAL) Enter the keyword `count` to count packets that the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes that the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DSCP values.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the `monitor` option.
6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *C9000 Series Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

Related Commands deny — Assigns a IP ACL filter to deny IP packets.

ip access-list standard — creates a standard ACL.

resequence access-list

Re-assign sequence numbers to entries in an existing ACL.

C9000 Series

Syntax resequence access-list {ipv4 | ipv6 | mac} {*access-list-name StartingSeqNum Step-to-Increment*}

Parameters

ipv4 | ipv6 | mac	Enter the keyword `ipv4`, `ipv6` or `mac` to identify the access-list type to resequence.
access-list-name	Enter the name of a configured ACL.
StartingSeqNum	Enter the starting sequence number to resequence. For IPv4 and IPv6 ACLs, the range is 0 to 4294967290; for MAC ACLs, the range is 0 to 65535.
Step-to-Increment	Enter the step to increment the sequence number. For IPv4 and IPv6 ACLs, the range is 0 to 4294967290; for MAC ACLs, the range is 0 to 65535.

Defaults The sequence number of ACL entries increases in multiples of 5; for example, seq 5, seq 10, seq 15 ...

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale (IPv6).
8.1.1.0	Introduced on the E-Series ExaScale (IPv4).
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing access-list.

Related Commands resequence prefix-list ipv4 — resequences a prefix list.

resequence prefix-list ipv4

Re-assign sequence numbers to entries of an existing prefix list.

C9000 Series

Syntax `resequence prefix-list ipv4 {prefix-list-name StartingSeqNum Step-to-increment}`

Parameters

prefix-list-name	Enter the name of the configured prefix list, up to 140 characters long.
StartingSeqNum	Enter the starting sequence number to resequence. The range is from 0 to 65535.
Step-to-Increment	Enter the step to increment the sequence number. The range is from 1 to 65535.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing prefix list.

Related Commands resequence access-list — resequences an access-list.

seq

Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

C9000 Series

Syntax

```
seq sequence-number {deny | permit} {source [mask] | any | host ip-address}}
[count [bytes]] [dscp value] [order] [fragments] [log [interval minutes]
[threshold-in-msgs [count]] [monitor]
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
source	Enter an IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
bytes	(OPTIONAL) Enter the keyword `bytes` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DSCP values. The range is from 0 to 63.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the `monitor` option.
6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *C9000 Series Configuration Guide*. The following conditions apply:

- The `seq` *`sequence-number`* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *`sequence-number`*.
- If *`sequence-number`* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *`sequence-number`* is configured, the sequence-number is used as a tie breaker for rules with the same order.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

Related Commands deny — configures a filter to drop packets.

permit — configures a filter to forward packets.

show ip access-lists

Display inbound or outbound IP access-list information based on a given option.

C9000 Series

Syntax `show ip access-lists {interface interface [in | out]}`

Parameters

interface Enter the keyword `interface` then one of the following keywords and slot/port or pe-id / stack-unit / port-id information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then the slot/port number.
- For a Port Channel interface, enter the keyword `port-channel` then a port channel number.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

in Enter the keyword `in` to display information for an ip ingress or inbound access-list attached to an interface.

out Enter the keyword `out` to display information for an ip egress or outbound access-list attached to an interface.

Defaults None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.

Usage Information If you do not attach an ingress or egress access-list to an interface, no information displays and you return to the `DELL#` prompt.

Example

```
Dell# show ip access-lists out
Standard Egress IP access list first
 seq 5 permit any count  bytes (0 bytes)
 seq 10 deny any count (0 packets)
Standard Egress  IP access list five
 seq 5 permit any
Standard Egress  IP access list four
 seq 5 permit any count  bytes (0 bytes)
 seq 10 deny any count (0 packets)
Standard Egress IP access list second
 seq 5 permit host 1.1.1.1 count  bytes (0 bytes)
Extended Egress  IP access list ten
 seq 5 permit tcp any eq 1 any
 seq 10 deny ip any host 11.11.11.11 count (0 packets)
```

Extended IP ACL Commands

The following commands configure extended IP ACLs, which in addition to the IP address, also examine the packet's protocol type. The C9000 supports both Ingress and Egress IP ACLs.

When an ACL is created without any rule and then applied to an interface, ACL behavior reflects an implicit permit.

NOTE: Also refer to the Commands Common to all ACL Types and Common IP ACL Commands sections.

deny

Configure a filter that drops IP packets meeting the filter criteria.

C9000 Series

Syntax

```
deny {ip | ip-protocol-number} {source mask | any | host ip-address}
{destination mask | any | host ip-address} [count [bytes]] [dscp value] [order]
[monitor] [fragments] [log [interval minutes] [threshold-in-msgs [count]]
[monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

ip	Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list denies all IP protocols.
ip-protocol-number	Enter a number from 0 to 255 to deny based on the protocol identified in the IP protocol header.
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.

destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets that the filter processes.
bytes	(OPTIONAL) Enter the keyword `byte` to count bytes that the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DSCP values. The range is from 0 to 63.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to include ACL matches in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *C9000 Series Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Related Commands

deny tcp — assigns a filter to deny TCP packets.

deny udp — assigns a filter to deny UDP packets.

ip access-list extended — creates an extended ACL.

deny icmp

To drop all or specific internet control message protocol (ICMP) messages, configure a filter.

C9000 Series

Syntax

```
deny icmp {source-ip-address mask | any | host ip-address} {destination mask | any | host ip-address} [log] [dscp] [[count [bytes]] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny icmp {source-ip-address mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source-ip-address	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
log	(OPTIONAL) Enter the keyword `log` to include ACL matches in the log.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword `bytes` to count bytes processed by the filter.

order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults

Not configured.

Command Modes

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword `dscp`.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
6.5.1.0	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *C9000 Series Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

ICMP Message Type Keywords	ICMP Message Type Name
administratively-prohibited	Administratively prohibited
alternate-address	Alternate host address
conversion-error	Datagram conversion error

ICMP Message Type Keywords	ICMP Message Type Name
dod-host-prohibited	Host prohibited
dod-net-prohibited	Net prohibited
echo	Echo
echo-reply	Echo reply
general-parameter-problem	Parameter problem
host-isolated	Host isolated
host-precedence-unreachable	Host unreachable for precedence
host-redirect	Host redirect
host-tos-redirect	Host redirect for TOS
host-tos-unreachable	Host unreachable for TOS
host-unknown	Host unknown
host-unreachable	Host unreachable
information-reply	Information replies
information-request	Information requests
mask-reply	Mask replies
mask-request	Mask requests
mobile-redirect	Mobile host redirect
net-redirect	Network redirect
net-tos-redirect	Network redirect for TOS
net-tos-unreachable	Network unreachable for TOS
net-unreachable	Network unreachable
network-unknown	Network unknown
no-room-for-option	Parameter required but no room
option-missing	Parameter required but not present
packet-too-big	Fragmentation needed and DF set
parameter-problem	All parameter problems
port-unreachable	Port unreachable
precedence-unreachable	Precedence cutoff
protocol-unreachable	Protocol unreachable
reassembly-timeout	Reassembly timeout
redirect	All redirects

ICMP Message Type Keywords	ICMP Message Type Name
router-advertisement	Router discovery advertisements
router-solicitation	Router discovery solicitations
source-quench	Source quenches
source-route-failed	Source route failed
time-exceeded	All time exceeded
timestamp-reply	Timestamp replies
timestamp-request	Timestamp requests
traceroute	Traceroute
ttl-exceeded	TTL exceeded
unreachable	All unreachables

deny tcp

Configure a filter that drops transmission control protocol (TCP) packets meeting the filter criteria.

C9000 Series

Syntax

```
deny tcp {source mask | any | host ip-address} [bit] [operator port [port]]
{destination mask | any | host ip-address} [dscp] [bit] [operator port [port]]
[count [bytes]] [order] [fragments] [log [interval minutes] [threshold-in-msgs
[count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
bit	Enter a flag or combination of bits: • `ack`: acknowledgement field • `fin`: finish (no more data from the user) • `psh`: push function

- `rst`: reset the connection
- `syn`: synchronize sequence numbers
- `urg`: urgent field

operator (OPTIONAL) Enter one of the following logical operand:

- `eq` = equal to
- `neq` = not equal to
- `gt` = greater than
- `lt` = less than
- `range` = inclusive range of ports (you must specify two ports for the `port` command)

port port Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535.

The following list includes some common TCP port numbers:

- 23 = Telnet
- 20 and 21 = FTP
- 25 = SMTP
- 169 = SNMP

destination Enter the IP address of the network or host to which the packets are sent.

mask Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.

count (OPTIONAL) Enter the keyword `count` to count packets the filter processes.

bytes (OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.

order (OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).

fragments Enter the keyword `fragments` to use ACLs to control packet fragments.

log (OPTIONAL) Enter the keyword `log` to include ACL matches in the log.

threshold-in msgs *count* (OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.

interval *minutes* (OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.

monitor (OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword `dscp`.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter in the *C9000 Series Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *C9000 Series Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Rule#  Data             Mask        From To #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule# Data               Mask             From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

deny — assigns a filter to deny IP traffic.

deny udp — assigns a filter to deny UDP traffic.

deny udp

To drop user datagram protocol (UDP) packets meeting the filter criteria, configure a filter.

C9000 Series

Syntax

```
deny udp {source mask | any | host ip-address} [operator port [port]]
{destination mask | any | host ip-address} [dscp] [operator port [port]] [count
[bytes]] [log] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny udp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
dscp	Enter this keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` command)
port port	Enter the application layer port number. Enter two port numbers if using the range logical operand. The range is from 0 to 65535.
destination	Enter the IP address of the network or host to which the packets are sent.

mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to include ACL matches in the log.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority) If you did not use the keyword `order`, the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword `dscp`.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter in the *C9000 Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *C9000 Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Rule#  Data              Mask        From To #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule# Data              Mask        From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

deny — assigns a filter to deny IP traffic.

deny tcp — assigns a filter to deny TCP traffic.

ip access-list extended

Configure an extended IP access list (IP ACL) based on IP addresses or protocols.

C9000 Series

Syntax

`ip access-list extended` *`access-list-name`* `[cpu-qos]`

To delete an access list, use the `no ip access-list extended` *`access-list-name`* `[cpu-qos]` command.

Parameters

access-list-name	Enter a string up to 140 characters long as the access list name.
cpu-qos	Enter the keyword `cpu-qos` to configure an extended IP ACL to be used only to filter protocol traffic for control-plane policing (CoPP).

Defaults

All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The number of entries allowed per ACL is hardware-dependent. For detailed information on the number entries allowed per ACL on the switch, refer to the Content Addressable Memory (CAM) chapter in the *C9000 Series Configuration Guide*.

If you configure an extended IP ACL to be used only to filter protocol traffic for CoPP, you must enter the keyword `cpu-qos`.

Use this command in Configuration Terminal Batch mode to configure the extended IP access list (IP ACL) in a dual-homing setup.

Example

```
Dell(conf)#ip access-list extended TESTListEXTEND
Dell(config-ext-nacl)#
```

Related Commands

ip access-list standard — configures a standard IP access list.

show config — displays the current configuration.

permit

To pass IP packets meeting the filter criteria, configure a filter.

C9000 Series

Syntax

`permit {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [bytes]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address in dotted decimal format of the network from which the packet was sent.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address or hostname.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword `bytes` to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DSCP values. The range is from 0 to 63.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the `monitor` option.
6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *C9000 Series Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

The software cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

Related Commands ip access-list extended — creates an extended ACL.

permit tcp — assigns a permit filter for TCP packets.

permit udp — assigns a permit filter for UDP packets.

permit icmp

Configure a filter to allow all or specific ICMP messages.

C9000 Series

Syntax

```
permit icmp {source mask | any | host ip-address} {destination mask | any | host ip-address} [dscp] [count [bytes]] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit icmp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or noncontiguous.
any	Enter the keyword `any` to match and drop specific Ethernet traffic on the interface.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is 0 to 63.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
bytes	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

Not configured.

Command Modes CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword `dscp`.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Added support for noncontiguous mask and added the `monitor` option.
6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *C9000 Series Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to Port Monitoring.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

permit tcp

To pass TCP packets meeting the filter criteria, configure a filter.

C9000 Series

Syntax

```
permit tcp {source mask | any | host ip-address} [bit] [operator port [port]]
{destination mask | any | host ip-address} [bit] [dscp] [operator port [port]]
[count [bytes]] [log] [order] [monitor] [fragments]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.

- Use the `no permit tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
bit	Enter a flag or combination of bits: • `ack`: acknowledgement field • `fin`: finish (no more data from the user) • `psh`: push function • `rst`: reset the connection • `syn`: synchronize sequence numbers • `urg`: urgent field
dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the port parameter)
port port	Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP • 169 = SNMP
destination	Enter the IP address of the network or host to which the packets are sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
bytes	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword `log` to include ACL matches in the log.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).

monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword `dscp`.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for non-contiguous mask and added the `monitor` option. Deprecated the keyword `established`.
6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter in the *C9000 Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *C9000 Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Rule# Data              Mask          From To   #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule# Data             Mask          From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

ip access-list extended — creates an extended ACL.

permit — assigns a permit filter for IP packets.

permit udp — assigns a permit filter for UDP packets.

permit udp

To pass UDP packets meeting the filter criteria, configure a filter.

C9000 Series

Syntax

`permit udp {`*`source mask`* `| any | host` *`ip-address`*`} [`*`operator port`* `[`*`port`*`]] {`*`destination mask`* `| any | host` *`ip-address`*`} [dscp] [`*`operator port`* `[`*`port`*`]] [count [bytes]] [order] [fragments] [log [interval` *`minutes`*`] [threshold-in-msgs [`*`count`*`]][monitor]`

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no permit udp {`*`source mask`* `| any | host` *`ip-address`*`} {`*`destination mask`* `| any | host` *`ip-address`* command.

Parameters

source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address.

dscp	Enter the keyword `dscp` to deny a packet based on the DSCP value. The range is from 0 to 63.
operator	(OPTIONAL) Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` parameter)
port port	Enter the application layer port number. Enter two port numbers if you are using the `range` logical operand. The range is 0 to 65535.
destination	Enter the IP address of the network or host to which the packets are sent.
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword `bytes` to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS priority for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to include ACL matches in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword `dscp`.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for non-contiguous mask and added the `monitor` option. .
6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *C9000 Series Configuration Guide*.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Most ACL rules require one entry in the CAM. However, rules with TCP and UDP port operators (for example, gt, lt, or range) may require more than one entry. The range of ports is configured in the CAM based on bit mask boundaries; the space required depends on exactly what ports are included in the range.

Example

An ACL rule with a TCP port range of 4000–8000 uses eight entries in the CAM.

```
Rule# Data              Mask          From To   #Covered

1 0000111110100000 1111111111100000 4000 4031 32
2 0000111111000000 1111111111000000 4032 4095 64
3 0001000000000000 1111100000000000 4096 6143 2048
4 0001100000000000 1111110000000000 6144 7167 1024
5 0001110000000000 1111111000000000 7168 7679 512
6 0001111000000000 1111111100000000 7680 7935 256
7 0001111100000000 1111111111000000 7936 7999 64
8 0001111101000000 1111111111111111 8000 8000 1

Total Ports: 4001
```

Example

An ACL rule with a TCP port lt 1023 uses only one entry in the CAM.

```
Rule# Data             Mask          From To   #Covered

1 0000000000000000 1111110000000000 0    1023 1024

Total Ports: 1024
```

Related Commands

ip access-list extended — creates an extended ACL.

permit — assigns a permit filter for IP packets.

permit tcp — assigns a permit filter for TCP packets.

resequence prefix-list ipv4

Re-assign sequence numbers to entries of an existing prefix list.

C9000 Series

Syntax

```
resequence prefix-list ipv4 {prefix-list-name StartingSeqNum Step-to-increment}
```

Parameters

prefix-list-name	Enter the name of the configured prefix list, up to 140 characters long.
StartingSeqNum	Enter the starting sequence number to resequence. The range is from 0 to 65535.
Step-to-Increment	Enter the step to increment the sequence number. The range is from 1 to 65535.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

When you have exhausted all the sequence numbers, this feature permits re-assigning a new sequence number to entries of an existing prefix list.

Related Commands

resequence access-list— resequences an access-list.

seq

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

C9000 Series

Syntax

```
seq sequence-number {deny | permit} {ip-protocol-number | icmp | ip | tcp |
udp} {source mask | any | host ip-address} {destination mask | any | host ip-
address} [operator port [port]] [count [byte] | [dscp value] [order]
[fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

Parameters

sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
ip-protocol-number	Enter a number from 0 to 255 to filter based on the protocol identified in the IP protocol header.
icmp	Enter the keyword `icmp` to configure an ICMP access list filter.
ip	Enter the keyword `ip` to configure a generic IP access list. The keyword `ip` specifies that the access list permits all IP protocols.
tcp	Enter the keyword `tcp` to configure a TCP access list filter.
udp	Enter the keyword `udp` to configure a UDP access list filter.
source	Enter an IP address in dotted decimal format of the network from which the packet was received.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D. The mask, when specified in A.B.C.D format, may be either contiguous or non-contiguous.
any	Enter the keyword `any` to specify that all routes are subject to the filter.
host *ip-address*	Enter the keyword `host` and then enter the IP address to specify a host IP address or hostname.
operator	(OPTIONAL) Enter one of the following logical operands: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt` = less than • `range` = inclusive range of ports (you must specify two ports for the `port` parameter.)
port port	(OPTIONAL) Enter the application layer port number. Enter two port numbers if you are using the range logical operand. The range is from 0 to 65535. The following list includes some common TCP port numbers: • 23 = Telnet • 20 and 21 = FTP • 25 = SMTP

- 169 = SNMP

destination	Enter the IP address of the network or host to which the packets are sent.
message-type	(OPTIONAL) Enter an ICMP message type, either with the type (and code, if necessary) numbers or with the name of the message type. The range is from 0 to 255 for ICMP type and from 0 to 255 for ICMP code.
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword `dcsp` to match to the IP DSCP values. The range is from 0 to 63.
order	(OPTIONAL) Enter the keyword `order` to specify the QoS order for the ACL entry. The range is from 0 to 254 (where 0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). If you do not use the keyword `order`, the ACLs have the lowest order by default (255).
fragments	Enter the keyword `fragments` to use ACLs to control packet fragments.
log	(OPTIONAL) Enter the keyword `log` to include ACL matches in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Add the DSCP value for ACL matching.
8.2.1.0	Allows ACL control of fragmented packets for IP (Layer 3) ACLs.
8.1.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added support for the non-contiguous mask and added the `monitor` option. Deprecated the keyword `established`.
6.5.10	Expanded to include the optional QoS `order` priority for the ACL entry.

Usage Information

If you configure the *sequence-number*, the *sequence-number* is used as a tie breaker for rules with the same order.

Use the `order` option only when you use policy-based QoS on the switch. For more information, refer to the Quality of Service chapter of the *C9000 Series Configuration Guide*. The following conditions apply:

- The `seq` *sequence-number* command is applicable only in an ACL group.
- The `order` option works across ACL groups that have been applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq` *sequence-number*.
- If *sequence-number* is not configured, the rules with the same order value are ordered according to their configuration order.
- If *sequence-number* is configured, the sequence-number is used as a tie breaker for rules with the same order.

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packets' details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny — configures a filter to drop packets.

permit — configures a filter to forward packets.

ACL VLAN Group Commands

Use the commands in this section to configure ACL VLAN groups and CAM optimization for ACLs applied to VLAN groups.

acl-vlan-group

Create an ACL VLAN group.

C9000 Series

Term heading	Description heading
Syntax	`acl-vlan-group` *`group name`* To remove an ACL VLAN group, use the `no acl-vlan-group` *`group name`* command.
Parameters	***group-name*** Enter the name of the ACL VLAN group (140 characters maximum).
Default	None
Command Modes	ACL-VLAN-GROUP CONFIGURATION CONFIGURATION TERMINAL BATCH

Command History

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S4810, S4820T, and Z9000.

Usage Information

You can configure up to eight different ACL VLAN groups at a time on the switch. When you configure an ACL VLAN group, you enter ACL VLAN Group configuration mode. You can also configure the ACL VLAN group in Configuration Terminal Batch mode that applies the configurations to the chassis in a dual-homing setup.

To avoid the problem of excessive consumption of CAM area, you can configure ACL VLAN groups that combines all the VLANs that are applied with the same ACL in a single group. A unique identifier for each of ACL attached to the VLAN is used as a handle or locator in the CAM area instead of the VLAN id. This method of processing significantly reduces the number of entries in the CAM area and saves memory space in CAM.

You can create an ACL VLAN group and attach the ACL with the VLAN members. Optimization is applicable only when you create an ACL VLAN group. If you apply an ACL separately on the VLAN interface, each ACL maps with the VLAN and increased CAM space utilization occurs.

Attaching an ACL individually to VLAN interfaces is similar to the behavior of ACL-VLAN mapping storage in CAM prior to the implementation of the ACL VLAN group functionality.

cam-acl-vlan

Configure the number of flow processor (FP) blocks of CAM allocated to ACL VLAN services on the switch.

C9000 Series

Syntax

```
cam-acl-vlan {default | vlanopenflow <0-2> | vlaniscsi <0-2> | vlanaclopt <0-2>}
```

Parameters

default	Reset the number of FP blocks to the default value. By default, 0 FP blocks of CAM are allocated for ACL VLAN services, such as iSCSI counters, Open Flow, and ACL VLAN optimization. **NOTE: CAM optimization for ACL VLAN groups is not enabled by default. You must allocate FP blocks of ACL VLAN CAM to enable ACL CAM optimization.**
vlanopenflow <0-2>	Allocate a number FP blocks of CAM for VLAN Open Flow operations.
vlaniscsi <0-2>	Allocate a number FP blocks of CAM for VLAN iSCSI counters.
vlanaclopt <0-2>	Allocate a number of FP blocks of CAM for CAM optimization of ACL VLAN operation.

Default

To reset the number FP blocks allocated for ACL VLAN processes, enter the `default` keyword with the `cam-acl-vlan` command. By default, 0 FP blocks are allocated for ACL VLAN operations on the switch.

Command Modes

ACL-VLAN-GROUP CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S4810 and Z9000.

Usage Information

The VLAN ContentAware Processor (VCAP) application is a pre-ingress CAP that modifies the VLAN settings before packets are forwarded. To support the ACL CAM optimization functionality, the CAM carving feature is enhanced. A total of four VACP groups are present, of which two are for fixed groups and the other two are for dynamic groups. Out of the total of two dynamic groups, you can allocate zero, one, or two flow processor (FP) blocks to iSCSI counters, Open Flow and ACL VLAN optimization. You can configure CAM FP blocks for only two of these ACL VLAN services at a time. Use this command in Configuration Terminal Batch mode to configure in a dual-homing setup.

description (ACL VLAN Group)

Add a text description of an ACL VLAN group.

C9000 Series

Syntax `description text`

Parameters

description	Enter a text to identify the ACL VLAN group (80 characters maximum).

Default No default behavior or values

Command Modes ACL-VLAN-GROUP CONFIGURATION (conf-acl-vl-grp)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S4810, S4820T, and Z9000.

Usage Information Enter a description for each ACL VLAN group that you create for effective administrative and logging purposes.

ip access-group (ACL VLAN Group)

Apply an egress IP ACL to the ACL VLAN group.

C9000 Series

Syntax `ip access-group access-list-name out implicit-permit`

Parameters

access-list-name	Enter the name of the egress IP ACL to be applied to member interfaces of the VLAN group (140 characters maximum).
out	Enter the keyword `out` to apply the ACL to outgoing traffic.
implicit-permit	Enter the keyword `implicit-permit` to change the default action of the ACL from implicit-deny to implicit-permit (that is, if the traffic does not match the filters in the ACL, the traffic is permitted instead of dropped).

Default None

Command Modes ACL-VLAN-GROUP CONFIGURATION (conf-acl-vl-grp)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.

Version	Description
9.3(0.0)	Introduced on the S4810, S4820T, and Z9000.

Usage Information You can apply only an egress IP ACL on an ACL VLAN group.

member vlan (ACL VLAN Group)

Add VLAN members to an ACL VLAN group.

C9000 Series

Syntax `member vlan {VLAN-range}`

Parameters

VLAN-range	Enter the member VLANs using comma-separated VLAN IDs, a range of VLAN IDs, a single VLAN ID, or a combination. For example: Comma-separated: 3, 4, 6 Range: 5-10 Combination: 3, 4, 5-10, 8

Default None

Command Modes ACL-VLAN-GROUP CONFIGURATION (conf-acl-vl-grp)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S4810, S4820T, and Z9000.

Usage Information At a maximum, there can be only 32 VLAN members in all ACL VLAN groups. A VLAN can belong to only one ACL VLAN group at a time.

You can create an ACL VLAN group and attach the ACL with the VLAN members. The optimization is applicable only when you create an ACL VLAN group. If you apply an ACL separately on the VLAN interface, each ACL has a mapping with the VLAN and increased CAM space utilization occurs.

Attaching an ACL individually to VLAN interfaces is similar to the behavior of ACL-VLAN mapping storage in CAM prior to the implementation of the ACL VLAN group functionality.

show acl-vlan-group

Display the configured ACL VLAN groups on the switch.

C9000 Series

Syntax `show acl-vlan-group {group-name | detail}`

Parameters

group-name	Display the configuration of an ACL VLAN group.
detail	Display information about all configured ACL VLAN groups in a line-by-line format.

Default No default behavior or values

Command Modes EXEC

EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S4810, S4820T, Z9000 and MXL.

Usage Information When an ACL VLAN group name or the access-list name contains more than 30 characters, the name is truncated in the show `show acl-vlan-group group-name` command output.

Examples The following example displays the output of the `show acl-vlan-group` command.

NOTE: Some group names and some access list names are truncated.

```
Dell#show acl-vlan-group
Group Name                    Egress IP Acl               Vlan Members
TestGroupSeventeenTwenty      SpecialAccessOnlyExperts    100,200,300
CustomerNumberIdentifica      AnyEmployeeCustomerEleve    2-10,99
HostGroup                     Group5                      1,1000
```

The following sample output shows the line-by-line style display when using the `show acl-vlan-group detail` option.

NOTE: No group or access list names are truncated

```
Dell#show acl-vlan-group detail

Group Name :
  TestGroupSeventeenTwenty
Egress IP Acl :
  SpecialAccessOnlyExpertsAllowed
Vlan Members :
  100,200,300

Group Name :
  CustomerNumberIdentificationEleven
Egress IP Acl :
```

```
  AnyEmployeeCustomerElevenGrantedAccess
Vlan Members :
  2-10,99

Group Name :
  HostGroup
Egress IP Acl :
  Group5
Vlan Members :
  1,1000
```

show cam-acl-vlan

Display the number of FP blocks of CAM that are allocated for different ACL VLAN services, including ACL VLAN optimization, VLAN iSCSI counters, and Open Flow.

C9000 Series

Syntax `show cam-acl-vlan`

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S4810, S4820T, Z9000 and MXL.

Usage Information After you allocate FP blocks of CAM to ACL VLAN operation, you must reboot the switch to enable ACL VLAN optimization.

The following table describes the output fields of the `show cam-acl-vlan` command:

Table 1. `show cam-acl-vlan` Command Description

Field	Description
Chassis Vlan Cam ACL	Details about the CAM blocks allocated for ACLs for various VLAN operations at a system-wide, global level.
Stack Unit <number>	Details about the CAM blocks allocated for ACLs for various VLAN operations for a particular stack unit.
Current Settings(in block sizes)	Information about the number of FP blocks that are currently in use or allocated.
VlanOpenFlow	Number of FP blocks for VLAN open flow operations.
VlanIscsi	Number of FP blocks for VLAN internet small computer system interface (iSCSI) counters.
VlanHp	Number of FP blocks for VLAN high performance processes.
VlanFcoe	Number of FP blocks for VLAN Fiber Channel over Ethernet (FCoE) operations.

Field	Description
VlanAclOpt	Number of FP blocks for ACL VLAN optimzation feature.

Example

```
Dell#show cam-acl-vlan
-- Chassis Vlan Cam ACL --
             Current Settings(in block sizes)
VlanOpenFlow :          0
VlanIscsi    :          2
VlanHp       :          1
VlanFcoe     :          1
VlanAclOpt :            0

-- Stack unit 0 --
           Current Settings(in block sizes)
VlanOpenFlow :          0
VlanIscsi    :          2
VlanHp       :          1
VlanFcoe     :          1
VlanAclOpt :            0
```

show running config acl-vlan-group

Display the running configuration of ACL VLAN groups.

C9000 Series

Syntax `show running config acl-vlan-group` *group-name*

Parameters

group-name	Display the specified ACL VLAN group (140 characters maximum).

Default None

Command Modes EXEC

EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S4810, S4820T, Z9000 and MXL.

Examples The following sample output shows the line-by-line style display when using the `show running-config acl-vlan-group` option. Note that no group or access list names are truncated.

```
Dell#show running-config acl-vlan-group
!
acl-vlan-group group1
 description Acl Vlan Group1
 member vlan 1-10,400-410,500
```

```
 ip access-group acl1 out implicit-permit
!
acl-vlan-group group2
 member vlan 20
 ip access-group acl2 out
Dell#

Dell#show running-config acl-vlan-group group1
!
acl-vlan-group group1
 description Acl Vlan Group1
 member vlan 1-10,400-410,500
 ip access-group acl1 out implicit-permit
```

Common MAC ACL Commands

The following commands are available within both MAC ACL modes (Standard and Extended) and do not have mode-specific options. These commands allow you to clear, display, and assign MAC ACL configurations.

The C9000 supports both Ingress and Egress MAC ACLs.

You can apply a MAC ACL on physical, port-channel and VLAN interfaces. The permit/deny statements in the ACL determine how traffic on an interface, VLAN members, or port-channel members is handled.

clear counters mac access-group

Clear counters for all or a specific MAC ACL.

C9000 Series

Syntax `clear counters mac access-group [mac-list-name]`

Parameters

mac-list-name	(OPTIONAL) Enter the name of a configured MAC access list.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

mac control-plane egress-acl

Enable user egress ACL for L2 control traffic on control plane.

C9000 Series

Syntax `mac control-plane egress-acl`

Parameters None

Defaults None

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Error Strings NONE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.

Usage Information Use this command in Configuration Terminal Batch mode to enable user egress ACL for L2 control traffic in a dual-homing setup.

mac access-group

Apply a MAC ACL to traffic entering or exiting an interface. You can apply a MAC ACL on a physical, port-channel, or VLAN interface.

C9000 Series

Syntax `mac access-group` *`access-list-name`* `{in [vlan` *`vlan-range`*`] | out}`

To delete a MAC access-group, use the `no mac access-group` *`mac-list-name`* command.

Parameters

access-list-name Enter the name of a configured MAC access list, up to 140 characters.

vlan *vlan-range*	(OPTIONAL) Enter the keyword `vlan` and then enter a range of VLANs. The range is from 1 to 4094 (you can use IDs 1 to 4094). **NOTE: This option is available only with the keyword`in` option.**
in	Enter the keyword `in` to configure the ACL to filter incoming traffic.
out	Enter the keyword `out` to configure the ACL to filter outgoing traffic.

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information You can assign one ACL (standard or extended) to an interface.

If you apply a MAC ACL on a VLAN:

- None of the VLAN members can have another ACL applied which has an entry for the VLAN.
- The VLAN cannot belong to an ACL VLAN group.

If you apply a MAC ACL on a physical or port-channel interface, a VLAN to which the port is associated cannot have another ACL applied.

If you apply a MAC ACL on an ACL VLAN group, none of the VLANs in the group can have another ACL applied.

Related Commands mac access-list standard — configures a standard MAC ACL.

mac access-list extended — configures an extended MAC ACL.

show mac access-lists

Display all of the Layer 2 ACLs configured in the system, whether or not they are applied to an interface, and the count of matches/ mismatches against each ACL entry displayed.

C9000 Series

Syntax `show mac access-lists [acl_name word | interface } {in | out | interface}`

Parameters

access-list	Displays information on all L2 access-lists configured.
acl_name *word*	Enter the acl_name *word* , up to 140 characters, for specified access-list.
interface *interface*	Enter the keyword `interface` then the one of the following keywords and slot/port or number information: • For a Port Channel interface, enter the keyword `port-channel` and then enter a number. The C-Series and S-Series range is from 1 to 4096. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` and then enter the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` and then enter the slot/port information. • For a VLAN interface, enter the keyword `VLAN` followed by the vlan id. • For a PE Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id/ stack-unit/ port-id* information. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.
in	Display information of L2 ingress access-list configured to an interface.
out	Display information of L2 egress access-list configured to an interface.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.4.1.0	Introduced.

Usage information

This command displays ingress or egress L2 access-list information based on a given option.

If no ingress or egress access-list is attached to an interface, no information displays and you return to the `DELL#` prompt.

Example

```
Dell#show mac access-lists in
Standard mac access list m1
 seq 5 permit 11:22:33:44:55:66 count (0 packets)
Standard mac access list m2
 seq 5 deny any order 2
 seq 10 permit 00:33:00:11:00:77 33:44:55:66:77:88 count (0 packets)
Extended mac access list m3
 seq 5 permit host  11:11:11:11:11:11 host  22:22:22:22:22:22  snap eq 600
Dell#
Dell#show mac access-lists out
Standard mac access list m1
 seq 5 permit 11:22:33:44:55:66 count (0 packets)
Standard mac access list m2
 seq 5 deny any order 2
 seq 10 permit 00:33:00:11:00:77 33:44:55:66:77:88 count (0 packets)
```

show mac accounting access-list

This command displays ACL Mac accounting information.

C9000 Series

Syntax

```
show mac accounting access-list {acl_name} {interface | cam_count}
```

Parameters

access-list	Display accounting information of all L2 access-lists configured.
acl_name	Display accounting information for specified access-list.
interface	Display accounting information for L2 access-list attached to a particular interface.
cam_count	Display accounting information of L2 access-lists with `cam_count`.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series
6.1.1.0	Introduced on the E-Series.

Usage Information

Displays occur only if the access-list is attached to an interface.

If no access-list is attached to the interface, no information displays and you are returned to the DELL# prompt.

Example

```
show mac accounting access-list
mac access-list standard mac
seq 5 permit 11:22:33:44:55:66 count
 seq 10 deny any log threshold-in-msgs 10 interval 5 order 1
 seq 15 permit any order 2 monitor
 !
```

Standard MAC ACL Commands

The following commands configure standard MAC ACLs. The C9000 supports both Ingress and Egress MAC ACLs.

When you create an access control list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit.

NOTE: For more information, also refer to the Commands Common to all ACL Types and Common MAC Access List Commands sections.

deny

To drop packets with a matching MAC address, configure a filter.

C9000 Series

Syntax

`deny {any | mac-source-address [mac-source-address-mask]} [count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no deny {any | mac-source-address mac-source-address-mask}` command.

Parameters

any	Enter the keyword `any` to specify that all routes are subject to the filter.

mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

Not enabled.

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the `monitor` option.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *C9000 Series Configuration Guide*.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

permit — configures a MAC address filter to pass packets.

seq — configures a MAC address filter with a specified sequence number.

mac access-list standard

To configure a standard MAC ACL, name a new or existing MAC access control list (MAC ACL) and enter MAC ACCESS LIST mode. Also refer to the Commands Common to all ACL Types section and the Common MAC Access List Commands section.

C9000 Series

Syntax

`mac access-list standard` *`mac-list-name`*

To delete a MAC access list, use the `no mac access-list standard` *`mac-list-name`* command.

Parameters

mac-list-name	Enter a text string as the name of the standard MAC access list (140 character maximum).

Defaults

Not configured.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The system supports one ingress and one egress MAC ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed information on the number entries allowed per ACL on the C9000, refer to the Content Addressable Memory (CAM) chapter in the *C9000 Configuration Guide*.

Use this command in Configuration Terminal Batch mode to configure a standard MAC ACL, name in a dual-homing setup.

Example

```
Dell(conf)#mac-access-list access-list standard TestMAC
Dell(config-std-macl)#?
deny              Specify packets to reject
description       List description
exit              Exit from access-list configuration mode
no                Negate a command or set its defaults
permit            Specify packets to forward
remark            Specify access-list entry remark
seq               Sequence numbers
show              Show Standard ACL configuration
```

permit

To forward packets from a specific source MAC address, configure a filter.

C9000 Series

Syntax

`permit {any | mac-source-address [mac-source-address-mask]} [count [byte]] | [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit {any | mac-source-address mac-source-address-mask}` command.

Parameters

any	Enter the keyword `any` to forward all packets received with a MAC address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.

threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

Not configured.

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *C9000 Series Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny — configures a MAC ACL filter to drop packets.

seq —configure a MAC ACL filter with a specified sequence number.

seq

To a deny or permit filter in a MAC access list while creating the filter, assign a sequence number.

C9000 Series

Syntax

`seq sequence-number {deny | permit} {any | mac-source-address [mac-source-address-mask]} [count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number from 0 to 65535.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition.
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this criteria.
any	Enter the keyword `any` to filter all packets.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of 00:00:00:00:00:00 is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

Not configured

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the `monitor` option.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *C9000 Series Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny — configures a filter to drop packets.

permit — configures a filter to forward packets.

Extended MAC ACL Commands

The following commands configure Extended MAC ACLs. The C9000 supports both Ingress and Egress MAC ACLs.
When an access-list is created without any rule and then applied to an interface, ACL behavior reflects implicit permit.

NOTE: For more information, also refer to the Commands Common to all ACL Types and Common MAC Access List Commands sections.

deny

To drop packets that match the filter criteria, configure a filter.

C9000 Series

Syntax

```
deny {any | host mac-address | mac-source-address mac-source-address-mask} {any
| host mac-address | mac-destination-address mac-destination-address-mask}
```

[*ethertype-operator*] [count [byte]] [log [interval *minutes*] [threshold-in-msgs [*count*]] [monitor]

To remove this filter, you have two choices:

- Use the `no seq` *sequence-number* command if you know the filter's sequence number.
- Use the `no deny {any | host` *mac-address* `|` *mac-source-address mac-source-address-mask*`} {any | host` *mac-address* `|` *mac-destination-address mac-destination-address-mask*`}` command.

Parameters

any	Enter the keyword `any` to drop all packets.
host *mac-address*	Enter the keyword `host` and then enter a MAC address to drop packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • `ev2` - is the Ethernet II frame format • `llc` - is the IEEE 802.3 frame format • `snap` - is the IEEE 802.3 SNAP frame format
count	(OPTIONAL) Enter the keyword `count` to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes processed by the filter.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults Not configured.

Command Modes CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the `monitor` option.
6.1.1.0	Introduced on the E-Series.

Usage Information When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *C9000 Series Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands permit — configures a MAC address filter to pass packets.

seq — configures a MAC address filter with a specified sequence number.

mac access-list extended

Configure an extended MAC access control list (extended MAC ACL).

C9000 Series

Syntax `mac access-list extended` *`access-list-name`* `[cpu-qos]`

To delete a MAC access list, use the `no mac access-list extended` *`access-list-name`* `[cpu-qos]` command.

Parameters

access-list-name	Enter a text string as the MAC access list name, up to 140 characters.
cpu-qos	Enter the keyword `cpu-qos` to configure an extended MAC ACL to be used only to filter protocol traffic for control-plane policing (CoPP).

Defaults none

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The number of entries allowed per ACL is hardware-dependent. For detailed specifications on entries allowed per ACL, refer to your line card documentation.

If you configure an extended MAC ACL to be used only to filter protocol traffic for CoPP, you must enter the keyword `cpu-qos`.

Use this command in Configuration Terminal Batch mode to configure an extended MAC access control list in a dual-homing setup.

Example

```
Dell(conf)#mac-access-list access-list extended TestMATExt
Dell(config-ext-macl)#remark 5 IPv4
Dell(config-ext-macl)#seq 10 permit any any ev2 eq 800 count bytes
Dell(config-ext-macl)#remark 15 ARP
Dell(config-ext-macl)#seq 20 permit any any ev2 eq 806 count bytes
Dell(config-ext-macl)#remark 25 IPv6
Dell(config-ext-macl)#seq 30 permit any any ev2 eq 86dd count bytes
Dell(config-ext-macl)#seq 40 permit any any count bytes
```

```
Dell(config-ext-macl)#exit
Dell(conf)#do show mac accounting access-list snickers interface te 0/47 in
Extended mac access-list snickers on TenGigabitEthernet 0/47
seq 10 permit any any ev2 eq 800 count bytes (559851886 packets 191402152148
bytes)
seq 20 permit any any ev2 eq 806 count bytes (74481486 packets 5031686754
bytes)
seq 30 permit any any ev2 eq 86dd count bytes (7751519 packets 797843521 bytes)
```

Related Commands

mac access-list standard — configures a standard MAC access list.

show mac accounting access-list — displays MAC access list configurations and counters (if configured).

permit

To pass packets matching the criteria specified, configure a filter.

C9000 Series

Syntax

`permit {any | host` *`mac-address`* `| mac-source-address mac-source-address-mask} {any | host` *`mac-address`* `| mac-destination-address mac-destination-address-mask} [ethertype operator] [count [byte]] | [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no permit {any | host` *`mac-address | mac-source-address mac-source-address-mask`*`} {any |` *`mac-destination-address mac-destination-address-mask`*`}` command.

Parameters

any	Enter the keyword `any` to forward all packets.
host	Enter the keyword `host` then a MAC address to forward packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes:

- `ev2` - is the Ethernet II frame format
- `llc` - is the IEEE 802.3 frame format
- `snap` - is the IEEE 802.3 SNAP frame format

count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

Not configured.

Command Modes

CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the `monitor` option.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter in the *C9000 Series Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny — configures a MAC ACL filter to drop packets.

seq — configure a MAC ACL filter with a specified sequence number.

seq

Configure a filter with a specific sequence number.

C9000 Series

Syntax

`seq` *`sequence-number`* `{deny | permit} {any | host` *`mac-address`* `| mac-source-address` *`mac-source-address-mask`*`} {any | host` *`mac-address`* `| mac-destination-address` *`mac-destination-address-mask`*`} [ethertype operator] [count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To delete a filter, use the `no seq` *`sequence-number`* command.

Parameters

sequence-number	Enter a number as the filter sequence number. The range is from zero (0) to 65535.
deny	Enter the keyword `deny` to drop any traffic matching this filter.
permit	Enter the keyword `permit` to forward any traffic matching this filter.
any	Enter the keyword `any` to filter all packets.
host *mac-address*	Enter the keyword `host` and then enter a MAC address to filter packets with that host address.
mac-source-address	Enter a MAC address in nn:nn:nn:nn:nn:nn format. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
mac-source-address-mask	Specify which bits in the MAC address must be matched.
mac-destination-address	Enter the destination MAC address and mask in nn:nn:nn:nn:nn:nn format.
mac-destination-address-mask	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of ff:ff:ff:ff:ff:ff allows entries that do not match and a mask of 00:00:00:00:00:00 only allows entries that match exactly.
ethertype operator	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes:

- `ev2` - is the Ethernet II frame format.
- `llc` - is the IEEE 802.3 frame format.
- `snap` - is the IEEE 802.3 SNAP frame format.

count	(OPTIONAL) Enter the keyword `count` to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword `byte` to count bytes the filter processes.
log	(OPTIONAL) Enter the keyword `log` to include ACL messages in the log.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface. For more information, refer to the "Flow-based Monitoring" section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

Defaults

Not configured.

Command Modes

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the `monitor` option.
6.1.1.0	Introduced on the E-Series.

Usage Information

When you use the `log` option, the CP processor logs detail the packets that match. Depending on how many packets match the log entry and at what rate, the CP may become busy as it has to log these packet details.

By default, 10 ACL logs are generated if you do not specify the threshold explicitly. The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Use the `monitor` option only when you are using flow-based monitoring. For more information, refer to the Port Monitoring chapter of the *C9000 Series Configuration Guide*.

NOTE: When ACL logging and byte counters are configured simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

Related Commands

deny — configures a filter to drop packets.

permit — configures a filter to forward packets.

IP Prefix List Commands

When you create an access-list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit.
To configure or enable IP prefix lists, use these commands.

clear ip prefix-list

Reset the number of times traffic meets the conditions ("hit" counters) of the configured prefix lists.

C9000 Series

Syntax

```
clear ip prefix-list [prefix-name]
```

Parameters

prefix-name	(OPTIONAL) Enter the name of the configured prefix list to clear only counters for that prefix list, up to 140 characters long.

Defaults

Clears "hit" counters for all prefix lists unless a prefix list is specified.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increase the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands ip prefix-list — configures a prefix list.

deny

To drop packets meeting the criteria specified, configure a filter.

C9000 Series

Syntax `deny ip-prefix [ge min-prefix-length] [le max-prefix-length]`

To delete a drop filter, use the `no deny ip-prefix` command.

Parameters

ip-prefix	Specify an IP prefix in the network/length format. For example, 35.0.0.0/ 8 means match the first 8 bits of address 35.0.0.0.
ge *min-prefix-length*	(OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.

Defaults Not configured.

Command Modes PREFIX-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

Related Commands permit — configures a filter to pass packets.

seq — configures a drop or permit filter with a specified sequence number.

ip prefix-list

Enter the PREFIX-LIST mode and configure a prefix list.

C9000 Series

Syntax

`ip prefix-list prefix-name`

To delete a prefix list, use the `no ip prefix-list prefix-name` command.

Parameters

prefix-name	Enter a string up to 16 characters long as the name of the prefix list, up to 140 characters long.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

Prefix lists redistribute OSPF and RIP routes meeting specific criteria.

Related Commands

show ip route list — displays IP routes in an IP prefix list.

show ip prefix-list summary — displays a summary of the configured prefix lists.

permit

Configure a filter that passes packets meeting the criteria specified.

C9000

Syntax

`permit` *`ip-prefix`* `[ge` *`min-prefix-length`*`] [le` *`max-prefix-length`*`]`

To delete a forward filter, use the `no permit` *`ip-prefix`* command.

Parameters

ip-prefix	Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
ge ***min-prefix-length***	(OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
le ***max-prefix-length***	(OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.

Command Modes

PREFIX-LIST

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

Sequence numbers for this filter are automatically assigned starting at sequence number 5.

If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

Related Commands

deny — configures a filter to drop packets.

seq — configures a drop or permit filter with a specified sequence number.

seq

To a deny or permit filter in a prefix list while configuring the filter, assign a sequence number.

C9000 Series

Syntax

`seq sequence-number {deny | permit} {any} | [ip-prefix /nn {ge min-prefix-length} {le max-prefix-length}] | [bitmask number]`

To delete a specific filter, use the `no seq sequence-number {deny | permit} {any} | [ip-prefix {ge min-prefix-length} {le max-prefix-length}] | [bitmask number]`.

Parameters

sequence-number	Enter a number. The range is from 1 to 65534.
deny	Enter the keyword `deny` to configure a filter to drop packets meeting this condition..
permit	Enter the keyword `permit` to configure a filter to forward packets meeting this condition.
any	(OPTIONAL) Enter the keyword `any` to match any packets.
ip-prefix /nn	(OPTIONAL) Specify an IP prefix in the network/length format. For example, 35.0.0.0/8 means match the first 8 bits of address 35.0.0.0.
ge *min-prefix-length*	(OPTIONAL) Enter the keyword `ge` and then enter the minimum prefix length, which is a number from zero (0) to 32.
le *max-prefix-length*	(OPTIONAL) Enter the keyword `le` and then enter the maximum prefix length, which is a number from zero (0) to 32.
bitmask *number*	Enter the keyword `bitmask` then enter a bit mask number in dotted decimal format.

Defaults

Not configured.

Command Modes

PREFIX-LIST

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.3.1.0	Added the `bit mask` option.

Usage Information If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

Related Commands deny — configures a filter to drop packets.

permit — configures a filter to pass packets.

show config

Display the current PREFIX-LIST configurations.

C9000 Series

Syntax `show config`

Command Modes PREFIX-LIST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell(conf-nprefixl)#show config
!
ip prefix-list snickers
Dell(conf-nprefixl)#
```

show ip prefix-list detail

Display details of the configured prefix lists.

C9000 Series

Syntax

```
show ip prefix-list detail [prefix-name]
```

Parameters

prefix-name	(OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip prefix-list detail
Prefix-list with the last deletion/insertion: filter_ospf
ip prefix-list filter_in:
count: 3, range entries: 3, sequences: 5 - 10
  seq 5 deny 1.102.0.0/16 le 32 (hit count: 0)
  seq 6 deny 2.1.0.0/16 ge 23 (hit count: 0)
  seq 10 permit 0.0.0.0/0 le 32 (hit count: 0)
ip prefix-list filter_ospf:
count: 4, range entries: 1, sequences: 5 - 10
  seq 5 deny 100.100.1.0/24 (hit count: 5)
  seq 6 deny 200.200.1.0/24 (hit count: 1)
  seq 7 deny 200.200.2.0/24 (hit count: 1)
  seq 10 permit 0.0.0.0/0 le 32 (hit count: 132)
Dell#
```

show ip prefix-list summary

Display a summary of the configured prefix lists.

C9000 Series

Syntax

```
show ip prefix-list summary [prefix-name]
```

Parameters

prefix-name	(OPTIONAL) Enter a text string as the name of the prefix list, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip prefix summary
Prefix-list with the last deletion/insertion: test
ip prefix-list test:
count: 3, range entries: 1, sequences: 5 - 15
ip prefix-list test1:
count: 2, range entries: 2, sequences: 5 - 10
ip prefix-list test2:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test3:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test4:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test5:
count: 1, range entries: 1, sequences: 5 - 5
ip prefix-list test6:
```

```
count: 1, range entries: 1, sequences: 5 - 5
Dell#
```

Route Map Commands

When you create an access-list without any rule and then apply the list to an interface, the ACL behavior reflects implicit permit.
To configure route maps and their redistribution criteria, use the following commands.

continue

To a route-map entry with a higher sequence number, configure a route-map.

C9000 Series

Syntax `continue [sequence-number]`

Parameters

sequence-number	(OPTIONAL) Enter the route map sequence number. The range is from 1 to 65535.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information The `continue` feature allows movement from one route-map entry to a specific route-map entry (the sequence number). If you do not specify the sequence number, the `continue` feature simply moves to the next sequence number (also known as an implied continue). If a match clause exists, the `continue` feature executes only after a successful match occurs. If there are no successful matches, the `continue` feature is ignored.

Match clause with Continue clause

The `continue` feature can exist without a match clause. A continue clause without a match clause executes and jumps to the specified route-map entry.

With a match clause and a continue clause, the match clause executes first and the continue clause next in a specified route map entry. The continue clause launches only after a successful match. The behavior is:

- A successful match with a continue clause, the route map executes the set clauses and then goes to the specified route map entry upon execution of the continue clause.
- If the next route map entry contains a continue clause, the route map executes the continue clause if a successful match occurs.
- If the next route map entry does not contain a continue clause, the route map evaluates normally. If a match does not occur, the route map does not continue and falls through to the next sequence number, if one exists.

Set Clause with Continue Clause

If the route-map entry contains sets with the continue clause, set actions are performed first then the continue clause jumps to the specified route map entry.

- If a set action occurs in the first route map entry and then the same set action occurs with a different value in a subsequent route map entry, the last set of actions overrides the previous set of actions with the same `set` command.
- If `set community additive` and `set as-path prepend` are configure, the communities and AS numbers are prepended.

Related Commands

set community — specifies a COMMUNITY attribute.

set as-path — configures a filter to modify the AS path.

description

Add a description to this route map.

C9000 Series

Syntax

`description {`*`description`*`}`

To remove the description, use the `no description {`*`description`*`}` command.

Parameters

description	Enter a description to identify the route map (80 characters maximum).

Defaults

none

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced.

Related Commands route-map — enables a route map.

match as-path

To match routes that have a certain AS number in their BGP path, configure a filter.

C9000 Series

Syntax `match as-path as-path-name`

To delete a match AS path filter, use the `no match as-path as-path-name` command.

Parameters

as-path-name	Enter the name of an established AS-PATH ACL, up to 140 characters.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands set as-path — adds information to the BGP AS_PATH attribute.

match community

To match routes that have a certain COMMUNITY attribute in their BGP path, configure a filter.

C9000 Series

Syntax

`match community` *`community-list-name`* `[exact]`

To delete a community match filter, use the `no match community` command.

Parameters

community-list-name	Enter the name of a configured community list.
exact	(OPTIONAL) Enter the keywords `exact` to process only those routes with this community list name.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

ip community-list — configures an Community Access list.

set community — specifies a COMMUNITY attribute.

neighbor send-community — sends COMMUNITY attribute to peer or peer group.

match interface

To match routes whose next hop is on the interface specified, configure a filter.

C9000 Series

Syntax

`match interface` *`interface`*

To remove a match, use the `no match interface` *`interface`* command.

Parameters

interface — Enter the following keywords and slot/port or number information:

- For the loopback interface, enter the keyword `loopback` then a number from zero (0) to 16383.
- For a Port Channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094 (you can use IDs 1 to 4094).

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

match ip address — redistributes routes that match an IP address.

match ip next-hop — redistributes routes that match the next-hop IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match metric — redistributes routes that match a specific metric.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match ip address

To match routes based on IP addresses specified in an access list, configure a filter.

C9000 Series

Syntax

`match ip address prefix-list-name`

To delete a match, use the `no match ip address prefix-list-name` command.

Parameters

prefix-list-name	Enter the name of configured prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip next-hop — redistributes routes that match the next-hop IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match metric — redistributes routes that match a specific metric.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match ip next-hop

To match based on the next-hop IP addresses specified in an IP access list or IP prefix list, configure a filter.

C9000 Series

Syntax

`match ip next-hop {prefix-list prefix-list-name}`

To delete a match, use the `no match ip next-hop {prefix-list prefix-list-name}` command.

Parameters

prefix-list *prefix-list-name*	Enter the keywords `prefix-list` and then enter the name of configured prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip address — redistributes routes that match an IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match metric — redistributes routes that match a specific metric.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match ip route-source

To match based on the routes advertised by routes specified in IP access lists or IP prefix lists, configure a filter.

C9000 Series

Syntax

`match ip route-source {prefix-list prefix-list-name}`

To delete a match, use the `no match ip route-source {prefix-list prefix-list-name}` command.

Parameters

prefix-list *prefix-list-name*	Enter the keywords `prefix-list` and then enter the name of configured prefix list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names were up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip address — redistributes routes that match an IP address.

match ip next-hop — redistributes routes that match the next-hop IP address.

match metric — redistributes routes that match a specific metric.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match metric

To match on a specified value, configure a filter.

C9000 Series

Syntax

`match metric` *`metric-value`*

To delete a value, use the `no match metric [`*`metric-value`*`]` command.

Parameters

metric-value	Enter a value to match. The range is from zero (0) to 4294967295.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip address — redistributes routes that match an IP address.

match ip next-hop — redistributes routes that match the next-hop IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match route-type — redistributes routes that match a route type.

match tag — redistributes routes that match a specific tag.

match origin

To match routes based on the value found in the BGP path ORIGIN attribute, configure a filter.

C9000 Series

Syntax

```
match origin {egp | igp | incomplete}
```

To disable matching filter, use the `no match origin {igp | egp | incomplete}` command.

Parameters

egp	Enter the keyword `egp` to match routes originating outside the AS.
igp	Enter the keyword `igp` to match routes originating within the same AS.
incomplete	Enter the keyword `incomplete` to match routes with incomplete routing information.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking TOS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
6.1.1.0	Introduced on the E-Series.

match route-type

To match routes based on the how the route is defined, configure a filter.

C9000 Series

Syntax

```
match route-type {external [type-1 | type-2] | internal | level-1 | level-2 | local}
```

To delete a match, use the `no match route-type {local | internal | external [type-1 | type-2] | level-1 | level-2}` command.

Parameters

external [type-1| type-2]	Enter the keyword `external` then either type-1 or type-2 to match only on OSPF Type 1 routes or OSPF Type 2 routes.
internal	Enter the keyword `internal` to match only on routes generated within OSPF areas.
level-1	Enter the keyword `level-1` to match IS-IS Level 1 routes.
level-2	Enter the keyword `level-2` to match IS-IS Level 2 routes.
local	Enter the keyword `local` to match only on routes generated within the switch.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip address — redistributes routes that match an IP address.

match ip next-hop — redistributes routes that match the next-hop IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match metric — redistributes routes that match a specific metric.

match tag — redistributes routes that match a specific tag.

match tag

To redistribute only routes that match a specified tag value, configure a filter.

C9000 Series

Syntax

`match tag tag-value`

To remove a match, use the `no match tag` command.

Parameters

tag-value	Enter a value as the tag on which to match. The range is from zero (0) to 4294967295.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

match interface — redistributes routes that match the next-hop interface.

match ip address — redistributes routes that match an IP address.

match ip next-hop — redistributes routes that match the next-hop IP address.

match ip route-source — redistributes routes that match routes advertised by other routers.

match metric — redistributes routes that match a specific metric.

match route-type — redistributes routes that match a route type.

route-map

Enable a route map statement and configure its action and sequence number. This command also places you in ROUTE-MAP mode.

C9000 Series

Syntax

`route-map` *map-name* `[permit | deny]` [*sequence-number*]

To delete a route map, use the `no route-map` *map-name* `[permit | deny]` [*sequence-number*] command.

Parameters

map-name	Enter a text string of up to 140 characters to name the route map for easy identification.
permit	(OPTIONAL) Enter the keyword `permit` to set the route map default as permit. If you do not specify a keyword, the default is `permit`.
deny	(OPTIONAL) Enter the keyword `deny` to set the route map default as deny.
sequence-number	(OPTIONAL) Enter a number to identify the route map for editing and sequencing with other route maps. You are prompted for a sequence number if there are multiple instances of the route map. The range is from 1 to 65535.

Defaults

Not configured.

If you do not define a keyword (`permit` or `deny`) for the route map, the `permit` action is the default.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information Use caution when you delete route maps because if you do not specify a sequence number, all route maps with the same *map-name* are deleted when you use the `no route-map map-name` command.

Example

```
Dell(conf)#route-map dempsey
Dell(config-route-map)#
```

Related Commands show config — displays the current configuration.

set as-path

To modify the AS path for border gateway protocol (BGP) routes, configure a filter.

C9000 Series

Syntax `set as-path prepend as-number [... as-number]`

To remove an AS-Path setting, use the `no set as-path {prepend as-number | tag}` command.

Parameters

prepend *as-number* Enter the keyword `prepend` and then enter up to eight AS numbers to be inserted into the BGP path information. The range is from 1 to 65535.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information You can prepend up to eight AS numbers to a BGP route.

This command influences best path selection in BGP by inserting a tag or AS number into the AS_PATH attribute.

Related Commands match as-path — redistributes routes that match an AS-PATH attribute.

ip as-path access-list — configures an AS-PATH access list.

neighbor filter-list — configures a BGP filter based on the AS-PATH attribute.

show ip community-lists — displays configured IP Community access lists.

set automatic-tag

To automatically compute the tag value of the route, configure a filter.

C9000 Series

Syntax

`set automatic-tag`

To return to the default, enter `no set automatic-tag`.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

set level — specify the OSPF area for route redistribution.

set metric — specify the metric value assigned to redistributed routes.

set metric-type — specify the metric type assigned to redistributed routes.

set tag — specify the tag assigned to redistributed routes.

set comm-list delete

To remove the specified community list from the BGP route's COMMUNITY attribute, configure a filter.

C9000 Series

Syntax

`set comm-list` *`community-list-name`* `delete`

To insert the community list into the COMMUNITY attribute, use the `no set comm-list` *`community-list-name`* `delete` command.

Parameters

community-list-name	Enter the name of an established Community list, up to 140 characters.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The community list used in the `set comm-list delete` command must be configured so that each filter contains only one community. For example, the filter `deny 100:12` is acceptable, but the filter `deny 120:13 140:33` results in an error.

If the `set comm-list delete` command and the `set community` command are configured in the same route map sequence, the deletion command (`set comm-list delete`) is processed before the insertion command (`set community`).

Related Commands

ip community-list — configures community access list.

match community — redistributes routes that match the COMMUNITY attribute.

set community — specifies a COMMUNITY attribute.

set community

Allows you to assign a BGP COMMUNITY attribute.

C9000 Series

Syntax

`set community {community-number | local-as | no-advertise | no-export | none} [additive]`

To delete a BGP COMMUNITY attribute assignment, use the `no set community {community-number | local-as | no-advertise | no-export | none}` command.

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system.
local-AS	Enter the keywords `local-AS` to drop all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to drop all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.
none	Enter the keyword `none` to remove the community attribute from routes meeting the route map criteria.
additive	(OPTIONAL) Enter the keyword `additive` to add the communities to already existing communities.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

ip community-list — configures community access list.

match community — redistributes routes that match the COMMUNITY attribute.

]neighbor send-community — assigns the COMMUNITY attribute.

show ip bgp community — displays BGP community groups.

show ip community-lists — displays configured Community access lists.

set level

To specify the IS-IS level or OSPF area to which matched routes are redistributed, configure a filter.

C9000 Series

Syntax

```
set level {backbone | level-1 | level-1-2 | level-2 | stub-area}
```

To remove a set level condition, use the `no set level {backbone | level-1 | level-1-2 | level-2 | stub-area}` command.

Parameters

backbone	Enter the keyword `backbone` to redistribute matched routes to the OSPF backbone area (area 0.0.0.0).
level-1	Enter the keyword `level-1` to redistribute matched routes to IS-IS Level 1.
level-1-2	Enter the keyword `level-1-2` to redistribute matched routes to IS-IS Level 1 and Level 2.
level-2	Enter the keyword `level-2` to redistribute matched routes to IS-IS Level 2.
stub-area	Enter the keyword `stub` to redistributed matched routes to OSPF stub areas.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

set automatic-tag — computes the tag value of the route.

set metric — specifies the metric value assigned to redistributed routes.

set metric-type — specifies the metric type assigned to redistributed routes.

set tag — specifies the tag assigned to redistributed routes.

set local-preference

To set the BGP LOCAL_PREF attribute for routers within the local autonomous system, configure a filter.

C9000 Series

Syntax

```
set local-preference value
```

To delete a BGP LOCAL_PREF attribute, use the `no set local-preference` command.

Parameters

value	Enter a number as the LOCAL_PREF attribute value. The range is from 0 to 4294967295.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The `set local-preference` command changes the LOCAL_PREF attribute for routes meeting the route map criteria. To change the LOCAL_PREF for all routes, use the `bgp default local-preference` command.

Related Commands bgp default local-preference — changes the default LOCAL_PREF attribute for all routes.

set metric

To assign a new metric to redistributed routes, configure a filter.

C9000 Series

Syntax `set metric [+ | -] metric-value`

To delete a setting, enter `no set metric`.

Parameters

+	(OPTIONAL) Enter + to add a metric-value to the redistributed routes.
-	(OPTIONAL) Enter – to subtract a metric-value from the redistributed routes.
metric-value	Enter a number as the new metric value. The range is from zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

set automatic-tag — computes the tag value of the route.

set level — specifies the OSPF area for route redistribution.

set metric-type — specifies the route type assigned to redistributed routes.

set tag — specifies the tag assigned to redistributed routes.

set metric-type

To assign a new route type for routes redistributed to OSPF, configure a filter.

C9000 Series

Syntax

```
set metric-type {internal | external | type-1 | type-2}
```

To delete a setting, use the `no set metric-type` command.

Parameters

internal	Enter the keyword `internal` to assign the Interior Gateway Protocol metric of the next hop as the route's BGP MULTI_EXIT_DES (MED) value.
external	Enter the keyword `external` to assign the IS-IS external metric.
type-1	Enter the keyword `type-1` to assign the OSPF Type 1 metric.
type-2	Enter the keyword `type-2` to assign the OSPF Type 2 metric.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.3.1.0	Implemented the keyword `internal`.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

set automatic-tag — computes the tag value of the route.

set level — specifies the OSPF area for route redistribution.

set metric — specifies the metric value assigned to redistributed routes.

set tag — specifies the tag assigned to redistributed routes.

set next-hop

To specify an IP address as the next hop, configure a filter.

C9000 Series

Syntax

`set next-hop` *ip-address*

To delete the setting, use the `no set next-hop` *ip-address* command.

Parameters

ip-address	Specify an IP address in dotted decimal format.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

If you configure the `set next-hop` command, its configuration takes precedence over the `neighbor next-hop-self` command in the ROUTER BGP mode.

If you configure the `set next-hop` command with the interface's IP address (either Loopback or physical), the software declares the route unreachable.

Related Commands

match ip next-hop — redistributes routes that match the next-hop IP address.

set origin

To manipulate the BGP ORIGIN attribute, configure a filter.

C9000 Series

Syntax

```
set origin {igp | egp | incomplete}
```

To delete an ORIGIN attribute setting, use the `no set origin` command.

Parameters

egp	Enter the keyword `egp` to set routes originating from outside the local AS.
igp	Enter the keyword `igp` to set routes originating within the same AS.
incomplete	Enter the keyword `incomplete` to set routes with incomplete routing information.

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.0	Introduced on the E-Series.

set tag

To specify a tag for redistributed routes, configure a filter.

C9000 Series

Syntax

```
set tag tag-value
```

To delete a setting, use the `no set tag` command.

Parameters

tag-value	Enter a number as the tag. The range is from zero (0) to 4294967295.

Defaults Not configured.

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

set automatic-tag — computes the tag value of the route.

set level — specifies the OSPF area for route redistribution.

set metric — specifies the metric value assigned to redistributed routes.

set metric-type — specifies the route type assigned to redistributed routes.

set weight

To add a non-RFC compliant attribute to the BGP route to assist with route selection, configure a filter.

C9000 Series

Syntax

`set weight weight`

To delete a weight specification, use the `no set weight weight` command.

Parameters

weight	Enter a number as the weight used by the route meeting the route map specification. The range is from 0 to 65535. The default is router-originated = **32768** and all other routes = **0**. When there are multiple routes to the same destination, the routes with a higher weight are preferred.

Defaults

router-originated = **32768**; all other routes = **0**

Defaults

Not configured.

Command Modes

ROUTE-MAP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

If you do not use the `set weight` command, router-originated paths have a weight attribute of 32768 and all other paths have a weight attribute of zero.

show config

Display the current route map configuration.

C9000 Series

Syntax `show config`

Command Modes ROUTE-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell(config-route-map)#show config
!
route-map hopper permit 10
Dell(config-route-map)#
```

show route-map

Display the current route map configurations.

C9000 Series

Syntax `show route-map [map-name]`

Parameters

map-name	(OPTIONAL) Enter the name of a configured route map, up to 140 characters.

Command Modes

- EXEC

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show route-map
route-map firpo, permit, sequence 10
 Match clauses:
 Set clauses:
  tag 34
Dell#
```

Related Commands

route-map — configures a route map.

AS-Path Commands

The following commands configure AS-Path ACLs.

ip as-path access-list

Enter AS-PATH ACL mode and configure an access control list based on the BGP AS_PATH attribute.

C9000 Series

Syntax

```
ip as-path access-list as-path-name
```

Parameters

as-path-name	Enter the access-list name, up to 140 characters.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
6.1.1.0	Introduced on the E-Series.

Usage Information

To apply the AS-PATH ACL to BGP routes, use the `match as-path` or `neighbor filter-list` commands.

Example

```
Dell(conf)#ip as-path access-list TestPath
Dell(config-as-path)#
```

Related Commands

match as-path — matches on routes contain a specific AS-PATH.

neighbor filter-list — configures filter based on AS-PATH information.

show ip as-path-access-lists

Display the all AS-PATH access lists configured on the E-Series.

C9000 Series

Syntax

```
show ip as-path-access-lists
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip as-path-access-lists
ip as-path access-list 1
 permit ^$
 permit ^\(.*\)$
 deny .*
ip as-path access-list 91
 permit ^$
 deny .*
 permit ^\(.*\)$
Dell#
```

IP Community List Commands

Use the following commands to configure IP community lists on the switch.

ip community-list

Enter COMMUNITY-LIST mode and create an IP community-list for BGP.

C9000 Series

Syntax

`ip community-list` *`comm-list-name`*

To delete a community-list, use the `no ip community-list` *`comm-list-name`* command.

Parameters

comm-list-name	Enter a text string as the name of the community-list, up to 140 characters.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, names are up to 16 characters long.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell(conf)#ip community-list TestComList
Dell(config-community-list)#
```

show ip community-lists

Display configured IP community lists in alphabetic order.

C9000 Series

Syntax `show ip community-lists [name]`

Parameters

name	(OPTIONAL) Enter the name of the standard or extended IP community list, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.

Example

```
Dell#show ip community-lists
ip community-list standard 1
 deny 701:20
 deny 702:20
 deny 703:20
 deny 704:20
 deny 705:20
 deny 14551:20
 deny 701:112
 deny 702:112
 deny 703:112
 deny 704:112
 deny 705:112
```

```
 deny 14551:112
 deny 701:666
 deny 702:666
 deny 703:666
 deny 704:666
 deny 705:666
 deny 14551:666
Dell#
```

7

Bidirectional Forwarding Detection (BFD)

Bidirectional forwarding detection (BFD) is a detection protocol that provides fast forwarding path failure detection.
The Dell Networking OS implementation is based on the standards specified in the IETF Draft draft-ietf-bfd-base-03.

Topics:

- bfd all-neighbors
- bfd disable
- bfd enable (Configuration)
- bfd enable (Interface)
- bfd interval
- bfd protocol-liveness
- ip route bfd
- ipv6 route bfd
- ip ospf bfd all-neighbors
- ipv6 ospf bfd all-neighbors
- neighbor bfd
- neighbor bfd disable
- show bfd neighbors
- vrrp bfd

bfd all-neighbors

Enable BFD sessions with all neighbors discovered by Layer 3 protocols virtual router redundancy protocol (VRRP), intermediate system to intermediate system (IS-IS), open shortest path first (OSPF), OSPFv3, or border gateway protocol (BGP) on router interfaces, and (optionally) reconfigure the default timer values.

C9000 Series

Syntax

```
[vrrp] bfd all-neighbors [interval interval min_rx min_rx multiplier value role
{active | passive}]
```

Parameters

vrrp	Enter the keyword `vrrp` in INTERFACE mode to enable BFD for VRRP.
interval *milliseconds*	(OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.
min_rx *milliseconds*	Enter the keyword `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 1000. The default is **200**.
multiplier *value*	Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.

role [active | passive]	Enter the role that the local system assumes: • `Active` — The active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **active**.

Defaults Refer to *Parameters*.

Command Modes

ROUTER OSPF

ROUTER OSPFv3

ROUTER BGP

ROUTER ISIS

INTERFACE (BFD for VRRP only)

Command History This guide is platform-specific. For command information about other platforms, see the to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(2.1P1)	Introduced support for enabling BFD on non-default VRFs for OSPFv2. Also, introduced support for enabling BFD on non-default VRFs for OSPFv3 .
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced BFD for VRRP and OSPFv3 on Z9000, S4810, and S4820T.
9.0.0.0	Introduced BFD for BGP on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced BFD for BGP on the S4810.
8.4.1.3	Introduced BFD for BGP on the E-Series ExaScale.
8.2.1.0	Introduced BFD for OSPF and ISIS on the E-Series ExaScale.
7.6.1.0	Introduced BFD for OSPF on the C-Series.
7.5.1.0	Introduced BFD for ISIS on the E-Series.
7.4.1.0	Introduced BFD for OSPF on the E-Series.

Usage Information All neighbors inherit the configured timer values except in the following cases:

- Timer values configured with the `isis bfd all-neighbors` or `ip ospf bfd all-neighbors` commands in INTERFACE mode override timer values configured with the `bfd all-neighbors` command. Likewise, using the `no bfd neighbor` command does not disable BFD on an interface if you explicitly enable BFD using the `isis bfd all-neighbors` command.
- Neighbors that have been explicitly enabled or disabled for a BFD session with the `bfd neighbor` or `neighbor bfd disable` commands in ROUTER BGP mode do not inherit the global BFD enable/disable

values configured with the `bfd all-neighbors` command or configured for the peer group to which a neighbor belongs. The neighbors inherit only the global timer values.

You can only enable BFD for VRRP in INTERFACE command mode (`vrrp bfd all-neighbors`).

Related Commands

show bfd neighbors — displays BFD neighbor information on all interfaces or a specified interface.

neighbor bfd disable — explicitly disables a BFD session with a BGP neighbor or a BGP peer group.

bfd disable

Disable BFD on an interface.

C9000 Series

Syntax

`bfd disable`

Re-enable BFD using the `no bfd disable` command.

Defaults

BFD is disabled by default.

Command Modes

VRRP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on S4810.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

bfd enable (Configuration)

Enable BFD on all interfaces.

C9000 Series

Syntax

```
bfd enable
```

Disable BFD using the `no bfd enable` command.

Defaults

BFD is disabled by default.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

bfd enable (Interface)

Enable BFD on an interface.

C9000 Series

Syntax

```
bfd enable
```

Defaults

BFD is enabled on all interfaces when you enable BFD from CONFIGURATION mode.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

bfd interval

Specify non-default BFD session parameters beginning with the transmission interval.

C9000 Series

Syntax `bfd interval` *`interval`* `min_rx` *`min_rx`* `multiplier` *`value`* `role {active | passive}`

Parameters

interval *milliseconds*	Enter the keywords `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is from 50 to 1000. The default is **200**.
multiplier *value*	Enter the keywords `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — The active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults Refer to *Parameters*.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell(conf-if-te-0/3)# bfd interval 250 min_rx 300 multiplier 4 role passive
Dell(conf-if-te-0/3)#
```

bfd protocol-liveness

Enable the BFD protocol liveness feature.

C9000 Series

Syntax `bfd protocol-liveness`

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
7.4.1.0	Introduced on the E-Series.

Usage Information Protocol Liveness is a feature that notifies the BFD Manager when a client protocol (for example, OSPF and ISIS) is disabled. When a client is disabled, all BFD sessions for that protocol are torn down. Neighbors on the remote system receive an Admin Down control packet and are placed in the Down state. Peer routers might take corrective action by choosing alternative paths for the routes that originally pointed to this router.

ip route bfd

Enable BFD for all neighbors configured through static routes.

Syntax

`ip route bfd [prefix-list` *`prefix-list-name`*`] [interval` *`interval`* `min_rx` *`min_rx`* `multiplier` *`value`* `role {active | passive}]`

To disable BFD for all neighbors configured through static routes, use the `no ip route bfd [prefix-list prefix-list-name] [interval` *`interval`* `min_rx` *`min_rx`* `multiplier` *`value`* `role {active | passive}]` command.

Parameters

prefix-list *prefix-list-name*	(Optional) Enter the keyword `prefix-list` followed by the name of the prefix list to enable or disable BFD on specific neighbors.
interval *milliseconds*	(OPTIONAL) Enter the keywords `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is **200**.
multiplier *value*	Enter the keywords `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults

See *Parameters*.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced the `prefix-list` keyword.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000–ON.
9.3.(0.0)	Introduced on S6000.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on Z9000, S4810, and S4820T.

Version	Description
8.2.1.0	Introduced on the E-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

ipv6 route bfd

Enable BFD for all IPv6 neighbors configured through static routes.

Syntax

`ipv6 route bfd [vrf vrf-name] [prefix-list prefix-list-name] [interval interval min_rx min_rx multiplier value role {active | passive}]`

To disable BFD for all IPv6 neighbors configured through static routes, use the `no ipv6 route bfd [vrf vrf-name] [prefix-list prefix-list-name] [interval interval min_rx min_rx multiplier value role {active | passive}]` command.

Parameters

vrf *vrf-name*	(Optional) Enter the keyword `vrf` and then the name of the VRF to enable or disable BFD on the next-hop IPv6 neighbor corresponding to that VRF.
prefix-list *prefix-list-name*	(Optional) Enter the keyword `prefix-list` followed by the name of the prefix list to enable or disable BFD on specific IPv6 neighbors.
interval *milliseconds*	(OPTIONAL) Enter the keywords `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is **200**.
multiplier *value*	Enter the keywords `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults See *Parameters*.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13(0.0)	Introduced on the S3100 series, S3048–ON, S4048–ON, S4048T-ON, S5000, S6000, S6000–ON, S6100–ON, C9010, and the Z9500.

Version	Description
9.12(1.0)	Introduced on the S5048F–ON.
9.11(2.5)	Introduced the `ipv6 route bfd` command on the Z9100–ON.

Example

```
DellEMC(conf)#ipv6 route bfd
DellEMC(conf)#ipv6 route bfd vrf vrf1 prefix-list p6_le
```

ip ospf bfd all-neighbors

Establish BFD sessions with all OSPF neighbors on a single interface or use non-default BFD session parameters.

Syntax

`ip ospf bfd all-neighbors [disable | [interval` *`interval`* `min_rx` *`min_rx`* `multiplier` *`value`* `role {active | passive}]]`

To disable all BFD sessions on an OSPF interface implicitly, use the `no ip ospf bfd all-neighbors disable` command in interface mode..

Parameters

disable	(OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.
interval *milliseconds*	(OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is **200**.
multiplier *value*	Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults

See *Parameters*.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.8(2.0)	Introduced on the S3100 series.
9.8(0.0P5)	Introduced on the S4048-ON.

Version	Description
9.8(0.0P2)	Introduced on the S3048-ON.
9.2.0.0	Introduced on the Z9000, S4820T, and S4810.

Usage Information

This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure `ip ospf bfd` in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the `bfd all-neighbors` command. Using the `no` form of this command does not disable BFD if you configure BFD in CONFIGURATION mode.

To disable BFD on a specific interface while you configure BFD in CONFIGURATION mode, use the keyword `disable`.

ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

C9000 Series

Syntax

`ipv6 ospf bfd all-neighbors [disable | [interval` *`interval`* `min_rx` *`min_rx`* `multiplier` *`value`* `role {active | passive}]]`

To disable all BFD sessions on an OSPFv3 interface implicitly, use the `no ipv6 ospf bfd all-neighbors disable` command in interface mode..

Parameters

disable	(OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.
interval *milliseconds*	(OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is **200**.
multiplier *value*	Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — The active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults See Parameters

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.0.0	Introduced on the Z9000, S4820T, and S4810.

Usage Information

This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure ipv6 ospf BFD in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the `bfd all-neighbors` command. Using the `no` form of this command does not disable BFD if you configure BFD in CONFIGURATION mode.

To disable BFD on a specific interface while you configure BFD in CONFIGURATION mode, use the keyword `disable`.

neighbor bfd

Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.

C9000 Series

Syntax

```
neighbor {ip-address | peer-group-name} bfd
```

Parameters

ip-address	Enter the IP address of the BGP neighbor that you want to explicitly enable for BFD sessions in dotted decimal format (A.B.C.D).
peer-group-name	Enter the name of the peer group that you want to explicitly enable for BFD sessions.

Defaults

none

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Version	Description
8.4.1.3	Introduced on the E-Series ExaScale.

Usage Information

When you enable a BFD session with a specified BGP neighbor or peer group using the `bfd all-neighbors` command, the default BFD session parameters are used (interval: **200** milliseconds, min_rx: **200** milliseconds, multiplier: **3** packets, and role: **active**) if you have not specified parameters with the `bfd all-neighbors` command.

When you explicitly enable a BGP neighbor for a BFD session with the `bfd neighbor` command:

- The neighbor does not inherit the global BFD enable values configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd all-neighbors` command: interval, min_rx, and multiplier.

Related Commands

neighbor bfd disable — explicitly disables a BFD session with a BGP neighbor or a BGP peer group.

show bfd neighbors — displays the BFD neighbor information on all interfaces or a specified interface.

neighbor bfd disable

Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.

C9000 Series

Syntax

```
neighbor {ip-address | peer-group-name} bfd disable
```

Parameters

ip-address	Enter the IP address of the BGP neighbor that you want to explicitly disable for BFD sessions in dotted decimal format (A.B.C.D).
peer-group-name	Enter the name of the peer group that you want to explicitly disable for BFD sessions.

Defaults

none

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, see to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Version	Description
8.4.1.3	Introduced on the E-Series ExaScale.

Usage Information

When you explicitly disable a BGP neighbor for a BFD session with the `neighbor bfd disable` command:

- The neighbor does not inherit the global BFD disable values configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd all-neighbors` command: interval, min_rx, and multiplier.

When you remove the Disabled state of a BFD for a BGP session with a specified neighbor by entering the `no neighbor bfd disable` command, the BGP link with the neighbor returns to normal operation and uses the BFD session parameters globally configured with the `bfd all-neighbors` command or configured for the peer group to which the neighbor belongs.

Related Commands

show bfd neighbors — displays the BFD neighbor information on all interfaces or a specified interface.

show bfd neighbors

Display BFD neighbor information on all interfaces or a specified interface.

C9000 Series

Syntax

```
show bfd [vrf vrf name] neighbors interface [detail]
```

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` then the slot/port information. • For a port-channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128. • For VLAN interfaces, enter the keyword `vlan` then a number from 1 to 4094. For ExaScale VLAN interfaces, the range is 1 to 2730 (VLAN IDs can be from 0 to 4093).
detail	(OPTIONAL) Enter the keyword `detail` to view detailed information about BFD neighbors.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(2.1P1)	Introduced the `vrf` keyword.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Added support for BFD for BGP on the S4810.
8.4.1.3	Added support for BFD for BGP on the E-Series ExaScale.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.5.1.0	Added support for BFD for VLAN and port-channel interfaces on the E-Series.
7.4.1.0	Introduced BFD on physical ports on the E-Series.

Example

```
Dell# show bfd neighbors

*    - Active session role
Ad Dn - Admin Down
B    - BGP
C    - CLI
I    - ISIS
O    - OSPF
R    - Static Route (RTM)

  LocalAddr  RemoteAddr  Interface State Rx-int Tx-int Mult Clients
* 10.1.3.2   10.1.3.1    Te 1/3    Up    300    250    3    C
```

Example (Detail)

```
Dell# show bfd neighbors detail

Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: TenGigabitEthernet 1/3
State: Up
Configured parameters:
 TX: 200ms, RX: 200ms, Multiplier: 3
Neighbor parameters:
 TX: 250ms, RX: 300ms, Multiplier: 4
Actual parameters:
 TX: 300ms, RX: 250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
 Number of packets received from neighbor: 376
 Number of packets sent to neighbor: 314
 Number of state changes: 2
 Number of messages from IFA about port state change: 0
 Number of messages communicated b/w Manager and Agent: 6
Dell#
```

Related Commands bfd all-neighbors — establishes BFD sessions with all neighbors discovered by the IS-IS protocol or OSPF protocol out of all interfaces.

vrrp bfd

Establish a BFD session with VRRP neighbors.

C9000 Series

Syntax

`vrrp bfd {all-neighbors | neighbor ip-address} [interval interval min_rx min_rx multiplier value role {active | passive}]`

To undo your VRRP BFD configuration, use the `no vrrp bfd {all-neighbors | neighbor ip-address } [interval interval min_rx min_rx multiplier value role {active | passive}]` command.

Parameters

all-neighbors	Establish BFD sessions with all BFD neighbors on an interface.
neighbor *ip-address*	Enter the IP address of the BFD neighbor.
interval *milliseconds*	(OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is 50 to 1000. The default is **200**.
min_rx *milliseconds*	Enter the keyword `min_rx` to specify the minimum rate at which the local system would like to receive control packets from the remote system. The range is 50 to 1000. The default is **200**.
multiplier	Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active`—The active system initiates the BFD session. Both systems can be active for the same session. • `Passive`—The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults See Parameters.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

Usage Information

When BFD is enabled with VRRP neighbors, the VRRP protocol registers with the BFD manager on the route processor. BFD sessions are established with all neighboring interfaces participating in VRRP. If a neighboring interface fails, the BFD agent on the line card notifies the BFD manager, which in turn notifies the VRRP protocol that a link state change occurred.

8

Border Gateway Protocol

BGP is an external gateway protocol that transmits interdomain routing information within and between autonomous systems (AS). BGP version 4 (BGPv4) supports classless inter-domain routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically sent messages to update those routing tables.

NOTE: For more information about configuring the border gateway protocol (BGP), see the *BGP* section in the *Dell EMC Networking OS Configuration Guide*.

Topics:

- BGP IPv4 Commands
- MBGP Commands
- BGP Extended Communities (RFC 4360)
- IPv6 BGP Commands
- IPv6 MBGP Commands

BGP IPv4 Commands

Border Gateway Protocol (BGP) is an external gateway protocol that transmits interdomain routing information within and between Autonomous Systems (AS). BGP supports classless interdomain routing (CIDR) and the aggregation of routes and AS paths. Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

address-family

Enable the IPv4 multicast or the IPv6 address family.

C9000 Series

Syntax `address-family {ipv4 [vrf vrf-name | multicast vrf vrf-name]| ipv6 unicast [vrf vrf-name]}`

Parameters

ipv4 multicast Enter the keyword `ipv4` followed by the keyword `multicast` to enable BGPv4 multicast mode.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added support for IPv6 VRF.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.5.1.0	Introduced

aggregate-address

To minimize the number of entries in the routing table, summarize a range of prefixes.

C9000 Series

Syntax

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

Parameters

ip-address mask	Enter the IP address and mask of the route to be the aggregate address. Enter the IP address in dotted decimal format (A.B.C.D) and mask in /prefix format (/x).
advertise-map *map-name*	(OPTIONAL) Enter the keywords `advertise-map` then the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keyword `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords `attribute-map` then the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keyword `summary-only` to advertise only the aggregate address. Specific routes are not advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords `suppress-map` then the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults

Not configured.

Command Modes

- ROUTER BGP ADDRESS FAMILY
- ROUTER BGP ADDRESS FAMILY IPv6

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

If routes within the aggregate are constantly changing, do not add the `as-set` parameter to the aggregate as the aggregate flaps to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is also true: routes meeting the `permit` clause are suppressed.

If the route is injected via the `network` command, that route still appears in the routing table if the `summary-only` parameter is configured in the `aggregate-address` command.

The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

In the `show ip bgp` command, aggregates contain an 'a' in the first column and routes suppressed by the aggregate contain an 's' in the first column.

When an aggregate address is denied using a peer's outbound route-map, individual routes suppressed by the aggregate address are advertised to that peer.

The attribute-map corresponding to an aggregate address is applied during the outbound update creation time; hence the value set in that attribute-map will not be shown in the output of the `show ip bgp aggregate route` command.

bgp add-path

Allow the advertisement of multiple paths for the same address prefix without the new paths replacing any previous ones.

C9000 Series

Syntax `bgp add-path [send | receive | both] path-count`

Parameters

send	Enter the keyword `send` to indicate that the system sends multiple paths to peers.
receive	Enter the keyword `receive` to indicate that the system accepts multiple paths from peers.
both	Enter the keyword `both` to indicate that the system sends and accepts multiple paths from peers.
path-count	(OPTIONAL) Enter the number paths supported. The range is from 2 to 64.

Defaults Disabled

Command Modes

- ROUTER BGP
- ROUTER BGP-address-family

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Related Commands neighbor add-path — specifies that this neighbor/peer group can send/receive multiple path advertisements.

bgp always-compare-med

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

C9000 Series

Syntax `bgp always-compare-med`

To disable comparison of MED, enter `no bgp always-compare-med`.

Defaults Disabled (that is, the software only compares MEDs from neighbors within the same AS).

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced command.
7.7.1.0	Introduced on the C-Series.

Usage Information Any update without a MED attribute is the least preferred route.

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp asnotation

Allows you to implement a method for AS number representation in the command line interface (CLI).

C9000 Series

Syntax `bgp asnotation [asplain | asdot+ | asdot]`

To disable a dot or dot+ representation and return to ASPLAIN, enter the `no bgp asnotation` command.

Defaults **asplain**

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.3.1.0	Introduced the dynamic application of AS notation changes
8.2.1.0	Introduced

Usage Information

Before enabling this feature, enable the `enable bgp four-octet-as-support`command. If you disable the `four-octect-support` command after using dot or dot+ format, the AS numbers revert to asplain text.

When you apply an asnotation, it is reflected in the running-configuration. If you change the notation type, the running-config updates dynamically and the new notation shows.

Example

```
Dell(conf)# router bgp 1
Dell(conf-router_bgp)# bgp asnotation asdot
Dell(conf-router_bgp)# ex
Dell(conf)# do show run | grep bgp

router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot

Dell(conf)#router bgp 1
Dell(conf-router_bgp)#bgp asnotation asdot+
Dell(conf-router_bgp)#ex

Dell(conf)#do show run | grep bgp
router bgp 1
  bgp four-octet-as-support
  bgp asnotation asdot+

Dell(conf)# router bgp 1
Dell(conf-router_bgp)#bgp asnotation asplain
Dell(conf-router_bgp)#ex
Dell(conf)#do show run |grep bgp
router bgp 1
  bgp four-octet-as-support

Dell(conf)#
```

Related Commands

bgp four-octet-as-support — enables 4-byte support for the BGP process.

bgp bestpath as-path ignore

Ignore the AS PATH in BGP best path calculations.

C9000 Series

Syntax

`bgp bestpath as-path ignore`

To return to the default, enter the `no bgp bestpath as-path ignore` command.

Defaults

Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath as-path multipath-relax

Include prefixes received from different AS paths during multipath calculation.

C9000 Series

Syntax `bgp bestpath as-path multipath-relax`

To return to the default BGP routing process, use the `no bgp bestpath as-path multipath-relax` command.

Defaults Disabled

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.4	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information The `bestpath router bgp configuration mode` command changes the default bestpath selection algorithm. The `multipath-relax` option allows load-sharing across providers with different (but equal-length) autonomous system paths. Without this option, ECMP expects the AS paths to be identical for load-sharing.

bgp bestpath med confed

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

C9000 Series

Syntax

`bgp bestpath med confed`

To disable MED comparison on BGP confederation paths, enter the `no bgp bestpath med confed` command.

Defaults

Disabled

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Inroduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The software compares the MEDs only if the path contains no external autonomous system numbers. If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath med missing-as-best

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over paths with an advertised MED attribute.

C9000 Series

Syntax

`bgp bestpath med missing-as-best`

To return to the default selection, use the `no bgp bestpath med missing-as-best` command.

Defaults

Disabled

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
6.3.1.0	Introduced

Usage Information

The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During path selection, paths with a lower MED are preferred over paths with a higher MED.

bgp bestpath router-id ignore

Do not compare router-id information for external paths during best path selection.

C9000 Series

Syntax

```
bgp bestpath router-id ignore
```

To return to the default selection, use the `no bgp bestpath router-id ignore` command.

Defaults

Disabled

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced

Usage Information Configuring this option retains the current best-path. When sessions are then reset, the oldest received path is chosen as the best-path.

bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

C9000 Series

Syntax `bgp client-to-client reflection`

To disable client-to-client reflection, use the `no bgp client-to-client reflection` command.

Defaults Enabled when a route reflector is configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information Route reflection to clients is not necessary if all client routers are fully meshed.

Related Commands bgp cluster-id — assigns an ID to a BGP cluster with two or more route reflectors.

neighbor route-reflector-client — configures a route reflector and clients.

bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

C9000 Series

Syntax `bgp cluster-id {ip-address | number}`

To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

Parameters

ip-address	Enter an IP address as the route reflector cluster ID.
number	Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors. Assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the cluster-id as an integer, it is displayed as an integer.

Related Commands bgp client-to-client reflection — enables route reflection between the route reflector and clients.

neighbor route-reflector-client — configures a route reflector and clients.

show ip bgp cluster-list — views paths with a cluster ID.

bgp confederation identifier

Configure an identifier for a BGP confederation.

C9000 Series

Syntax `bgp confederation identifier` *`as-number`*

To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

Parameters

as-number	Enter the AS number. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series. Added support for the 4-byte format

Usage Information To accept 4-byte formats before entering a 4-byte AS number, configure your system. All the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

The system accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

Related Commands bgp four-octet-as-support — enables 4-byte support for the BGP process.

bgp confederation peers

Specify the autonomous systems (ASs) that belong to the BGP confederation.

C9000 Series

Syntax `bgp confederation peers` *as-number* `[...as-number]`

To return to the default, use the `no bgp confederation peers` command.

Parameters

as-number	Enter the AS number. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

...as-number	(OPTIONAL) Enter up to 16 confederation numbers. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series. Added support for the 4-byte format.

Usage Information All the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems.

After specifying autonomous systems numbers for the BGP confederation, recycle the peers to update their configuration.

This command automatically restarts the BGP instance for the configuration to take effect.

Related Commands bgp confederation identifier — configures a confederation ID.

bgp four-octet-as-support — enables 4-byte support for the BGP process.

bgp dampening

Enable BGP route dampening and configure the dampening parameters.

C9000 Series

Syntax `bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]`

To disable route dampening, use the `no bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]` command.

Parameters

half-life	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. The range is from 1 to 45. The default is **15 minutes**.
reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is from 1 to 20000. The default is **750**.
suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is from 1 to 20000. The default is **2000**.
max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is from 1 to 255. The default is **60 minutes**.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` then the name of a configured route map. Only `match` commands in the configured route map are supported.

Defaults Disabled.

Command Modes

- ROUTER BGP
- ROUTER BGP-address-family

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information If you enter the `bgp dampening` command, the default values for *`half-life`*, *`reuse`*, *`suppress`*, and *`max-suppress-time`* are applied. The parameters are position-dependent; therefore, if you configure one parameter, configure the parameters in the order they appear in the CLI.

Related Commands show ip bgp dampened-paths — views the BGP paths.

bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

C9000 Series

Syntax

```
bgp default local-preference value
```

To return to the default value, use the `no bgp default local-preference` command.

Parameters

value	Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. The range is from 0 to 4294967295. The default is **100**.

Defaults **100**

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information All routers apply the `bgp default local-preference` command setting within the AS. To set the local preference for a specific route, use the `set local-preference` command in ROUTE-MAP mode.

Related Commands set local-preference — assigns a local preference value for a specific route.

bgp dmzlink-bw

Enable BGP Link Bandwidth.

C9000 Series

Syntax

```
bgp dmzlink-bw
```

To disable BGP Link Bandwidth, enter the `no bgp dmzlink-bw` command.

Parameters

dmzlink-bw	Enter the keyword `dmzlink-bw` to enable BGP Link Bandwidth in BGP multipath.

Defaults N/A

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010 Series.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S-Series.

Usage Information

Configuring or un-configuring the command will bring down and bring up the BGP Route Manager, this will result in tear down and re-establishment of all active sessions.

Link Bandwidth has to be configured on the router in order to tell it to associate Link Bandwidth with prefixes (paths) and/or to use Link Bandwidth in BGP Multipath route selection.

This is done under BGP configuration and is supported per address family – for IPv4 and IPv6 address families.

The configuration for a particular address family will apply across all VRFs configured.

This command must be performed on the router which is attaching link bandwidth to prefixes (typically a border router) as well as the router which is expected to load share traffic proportional to the bandwidth of the external links.

bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

C9000 Series

Syntax `bgp enforce-first-as`

To turn off the default, use the `no bgp enforce-first-as` command.

Defaults Enabled

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

Usage Information

This command is enabled by default, that is for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is increments. Use the `show ip bgp neighbors` command to view the "failed enforce-first-as check" counter.

If you disable the `enforce-first-as` command, it can be viewed using the `show ip protocols` command.

Related Commands

show ip bgp neighbors — views the information the BGP neighbors exchange.

show ip protocols — views information on routing protocols.

bgp fast-external-fallover

Enable the fast external fallover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

C9000 Series

Syntax

```
bgp fast-external-fallover
```

To disable fast external fallover, use the `no bgp fast-external-fallover` command.

Defaults

Enabled

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Version	Description
7.7.1.0	Introduced on the C-Series.

Usage Information The `bgp fast-external-fallover` command appears in the `show config` command output.

bgp four-octet-as-support

Enable 4-byte support for the BGP process.

C9000 Series

Syntax `bgp four-octet-as-support`

To disable fast external failover, use the `no bgp four-octet-as-support` command.

Defaults Disabled (supports 2–byte format)

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information Routers supporting 4-byte ASNs advertise that function in the OPEN message. The behavior of a 4-byte router is slightly different depending on whether it is speaking to a 2-byte router or a 4-byte router.

When creating Confederations, all the routers in the Confederation must be 4 byte or 2 byte identified routers. You cannot mix them.

Where the 2-byte format is from 1 to 65535, the 4-byte format is from 1 to 4294967295. Both formats are accepted and the advertisements reflect the entered format.

For more information about using the 2 byte or 4-byte format, refer to the *Dell Networking OS Configuration Guide*.

bgp graceful-restart

To support graceful restart as a receiver only, enable graceful restart on a BGP neighbor, a BGP node, or designate a local router.

C9000 Series

Syntax

`bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]`

To return to the default, use the `no bgp graceful-restart` command.

Parameters

restart-time *seconds*	Enter the keyword `restart-time` then the maximum number of seconds to restart and bring-up all the peers. The range is from 1 to 3600 seconds. The default is **120 seconds**.
stale-path-time *seconds*	Enter the keyword `stale-path-time` then the maximum number of seconds to wait before restarting a peer's stale paths. The default is **360 seconds**.
role receiver-only	Enter the keyword `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults

as above

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

BGP graceful restart is active only when the neighbor becomes established. Otherwise it is disabled. Graceful-restart applies to all neighbors with established adjacency.

bgp log-neighbor-changes

Enable logging of BGP neighbor resets.

C9000 Series

Syntax

```
bgp log-neighbor-changes
```

To disable logging, use the `no bgp log-neighbor-changes` command.

Defaults Enabled

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To view BGP neighbor resets, use the `show logging` command in EXEC mode.

The `bgp log-neighbor-changes` command appears in the `show config` command output.

Related Commands show logging — views logging settings and system messages logged to the system.

bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems.

C9000 Series

Syntax

```
bgp non-deterministic-med
```

To return to the default, use the `no bgp non-deterministic-med` command.

Defaults Disabled (that is, paths/routes for the same destination but from different ASs do not have their MEDs compared).

Command Modes ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

In Non-Deterministic mode, paths are compared in the order in which they arrive. This method can lead the system to choose different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (`no bgp non-deterministic-med`), the system compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS.

When you change the path selection from Deterministic to Non-Deterministic, the path selection for the existing paths remains Deterministic until you enter the `clear ip bgp` command to clear existing paths.

bgp outbound-optimization

Enables outbound optimization for IBGP peer-group members.

Syntax

`bgp outbound-optimization`

To disable outbound optimization, enter the `no bgp outbound-optimization` command.

Defaults

Enabled.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.4.(0.0)	Introduced on the S4810.
9.2(1.0)	Introduced on the Z9500.

Usage Information

The updates are sent to all the neighbors in the peer-group and all the neighbors have the same attributes including next-hop.

Enabling or disabling outbound optimization dynamically resets all neighbor sessions.

When you enable outbound optimization, all peers receive the same update packets. Also, the next-hop address, which is chosen as one of the addresses of the neighbor's reachable interface, is the same for all peers.

bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

C9000 Series

Syntax

`bgp recursive-bgp-next-hop`

To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

Defaults

Enabled

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.2.1.0	Introduced.

Usage Information

This command is a *knob* to disable BGP next-hop resolution using BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not.

The `clear ip bgp` command is required for this command to take effect and to keep the BGP database consistent. Execute the `clear ip bgp` command right after executing this command.

Related Commands

clear ip bgp — clears the ip bgp.

bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

C9000 Series

Syntax

`bgp regex-eval-optz-disable`

To re-enable optimization engine, use the `no bgp regex-eval-optz-disable` command.

Defaults

Enabled

Command Modes

ROUTER BGP (conf-router_bgp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced

Usage Information

BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is common. In a large-scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.

BGP policies, containing regular expressions to match as-path and communities, tend to use much CPU processing time, which in turn affects the BGP routing convergence. Additionally, the `show bgp` commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The Regex Engine Performance Enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expensive of RP1 processor memory.

Examples

```
Dell(conf-router_bgp)# no bgp regex-eval-optz-disable
Dell(conf-router_bgp)# do show ip protocols
Routing Protocol is "ospf 22222"
  Router ID is 2.2.2.2
  Area              Routing for Networks
  51                10.10.10.0/00

Routing Protocol is "bgp 1"
  Cluster Id is set to 10.10.10.0
  Router Id is set to 10.10.10.0
```

```
  Fast-external-fallover enabled
Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
    BGP table version is 0, main routing table version 0
    Distance: external 20 internal 200 local 200

Dell(conf-router_bgp)#
```

Related Commands show ip protocols — views information on all routing protocols enabled and active on the E-Series.

bgp router-id

Assign a user-given ID to a BGP router.

C9000 Series

Syntax `bgp router-id ip-address`

To delete a user-assigned IP address, use the `no bgp router-id` command.

Parameters

ip-address	Enter an IP address in dotted decimal format to reset only that BGP neighbor.

Defaults The router ID is the highest IP address of the Loopback interface or, if no Loopback interfaces are configured, the highest IP address of a physical interface on the router.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information Peering sessions are reset when you change the router ID of a BGP router.

bgp soft-reconfig-backup

To avoid the peer from resending messages, use this command *only* when route-refresh is *not* negotiated.

C9000 Series

Syntax

```
bgp soft-reconfig-backup
```

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

Defaults

Off

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for IPv6.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.2.1.0	Introduced.

Usage Information

When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

Related Commands

clear ip bgp — activates inbound policies without resetting the BGP TCP session.

capture bgp-pdu neighbor

Enable capture of an IPv4 BGP neighbor packet.

C9000 Series

Syntax

`capture bgp-pdu neighbor` *`ipv4-address`* `direction {both | rx | tx}`

To disable capture of the IPv4 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv4-address` command.

Parameters

ipv4-address	Enter the IPv4 address of the target BGP neighbor.
direction {both | rx | tx}	Enter the keyword `direction` and a direction — either `rx` for inbound, `tx` for outbound, or both.

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced.

Related Commands

capture bgp-pdu max-buffer-size — specifies a size for the capture buffer.

show capture bgp-pdu neighbor — displays BGP packet capture information.

capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

C9000 Series

Syntax `capture bgp-pdu max-buffer-size 100-102400000`

Parameters

100-102400000 Enter a size for the capture buffer.

Defaults **40960000 bytes.**

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced

Related Commands capture bgp-pdu neighbor — enables capture of an IPv4 BGP neighbor packet.

show capture bgp-pdu neighbor — displays BGP packet capture information for an IPv6 address on the E-Series.

clear ip bgp

Reset BGP sessions. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

C9000 Series

Syntax

```
clear ip bgp [vrf vrf-name] [* | <1-4294967295> | <0.1-65535.65535> | A.B.C.D
{soft {in | out}} | X:X:X:X::X {soft {in | out}} | dampening | flap-statistics
| ipv4 | ipv6 | peer-group]
```

Parameters

vrf *vrf-name*	Enter the keyword `vrf` and then the name of the VRF to clear all BGP sessions corresponding to that VRF. **NOTE: Use this attribute to clear a BGP instance corresponding to either a specific address family in a default VRF or an IPv4 address family in a a non-default VRF.**
*	Enter an asterisk (*) to reset all BGP sessions.
<1-4294967295>	Enter <1-4294967295> to clear peers with the AS number.
<0.1-65535.65535>	Enter <0.1-65535.65535> to clear peers with the AS number in dot format.
A.B.C.D	Enter the BGP neighbor address in the A.B.C.D format to clear.
X:X:X:X::X	Enter the BGP neighbor address in the X:X:X:X::X format to clear.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. **NOTE: If you enter the `clear ip bgp ip-address soft` command, both inbound and outbound policies are reset.**
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies. **NOTE: You must execute the `clear ip bgp soft out` command when ever there is a change in the local policy. If you do not run this command after a local policy change, then these policy changes are not reflected in the responses to the peer's route refresh messages.**
dampening	Enter the keyword `dampening` to clear the flap dampening information.
flap-statistics	Enter the keywords `flap-statistics` to clear the flap statistics information.
ipv4	Enter the ipv4 address family to clear.
ipv6	Enter the ipv6 address family to clear.
peer-group	Enter the peer-group to clear all members of the peer-group.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
6.5.1.0	Expanded to include the `as-number` option.

Related Commands bgp recursive-bgp-next-hop — disables next-hop resolution through other routes learned by the BGP.

clear ip bgp dampening

Clear information on route dampening and return the suppressed route to the Active state.

C9000 Series

Syntax

```
clear ip bgp [vrf vrf-name] [ipv4 [multicast | unicast] | ipv6 unicast]
[dampening [ipv4-address mask | ipv6-address mask]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to clear information on route dampening corresponding to that VRF **NOTE: You can use this attribute on a specific VRF to remove history routes corresponding to that VRF. You can also use this attribute to return the suppressed routes corresponding to a specific VRF to an active state.**
ipv4 multicast	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to clear the ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to clear the ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to clear the ipv6 unicast routes.
ipv4-address mask	(OPTIONAL) Enter an IPv4 address in dotted decimal format and the prefix mask in slash format (/x) to clear dampening information only that BGP neighbor.
ipv6–address mask	(OPTIONAL) Enter the IPv6 address and the network mask to clear information on IPv6 route dampening.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.

Version	Description
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

After you enter this command, the software deletes the history routes and returns the suppressed routes to the Active state.

The `clear ip bgp dampening` command does not clear the history paths.

clear ip bgp flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

C9000 Series

Syntax

```
clear ip bgp [vrf vrf-name] [ipv4 [multicast | unicast] | ipv6 unicast] [flap-statistics [ipv4-address mask | ipv6-address mask] | filter-list as-path-name | regexp regular-expression]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to clear BGP flap statistics corresponding to that VRF. **NOTE: You can use this attribute on a specific VRF to remove history routes corresponding to that VRF. You can also use this attribute to return the suppressed routes corresponding to a specific VRF to an active state.**
ipv4 multicast	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to clear information related only to ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to clear information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to clear information related only to ipv6 unicast routes.
ipv4-address mask	(OPTIONAL) Enter an IPv4 address in dotted decimal format and the prefix mask in slash format (/x) to reset only that prefix.
ipv6–address mask	(OPTIONAL) Enter the IPv6 address followed by the network mask to reset only that prefix.
filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` then the name of a configured AS-PATH list.

regexp *regular-expression*

(OPTIONAL) Enter the keyword `regexp` then regular expressions. Use one or a combination of the following:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (0 or more sequences).
- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

  NOTE: Enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
- `[ ]` = (brackets) a range of single-character patterns.
- `( )` = (parenthesis) groups a series of pattern elements to a single element.
- `{ }` = (braces) minimum and the maximum match count.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

If you enter the `clear ip bgp flap-statistics` command without any parameters, all statistics are cleared.

Related Commands

show debugging — views the enabled debugging operations.

show ip bgp flap-statistics — views the BGP flap statistics.

undebug all — disables all debugging operations.

clear ip bgp peer-group

Reset a peer-group's BGP sessions.

C9000 Series

Syntax

```
clear ip bgp [vrf vrf-name] peer-group peer-group-name [ipv4 [multicast | unicast] | ipv6 unicast] [soft {in | out}]
```

Parameters

vrf *vrf-name*	Enter the keyword `vrf` and then the name of the VRF to reset the peer group corresponding to that VRF. **NOTE: You can use this attribute on a specific VRF to remove history routes corresponding to that VRF. You can also use this attribute to return the suppressed routes corresponding to a specific VRF to an active state.**
peer-group-name	Enter the peer group name to reset the BGP sessions within that peer group.
ipv4 multicast	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to reset ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to reset ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to reset ipv6 unicast routes.
soft	(OPTIONAL) Enter the keyword `soft` to reset soft configuration.
in	Enter the keyword in to re-configure soft inbound updates.
out	Enter the keyword out to re-configure soft outbound updates.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Version	Description
7.7.1.0	Introduced on the C-Series.

debug ip bgp

Display all information on BGP, including BGP events, keepalives, notifications, and updates.

C9000 Series

Syntax

`debug ip bgp [ vrf vrf-name | A.B.C.D | X:X:X:X::X | peer-group peer-group-name] [in | out]`

To disable all BGP debugging, use the `no debug ip bgp` command.

Parameters

vrf *vrf-name*	Enter the keyword `vrf` and then the name of the VRF to debug BGP information corresponding to that VRF. **NOTE: Use this attribute to debug BGP protocol operations corresponding to either a default or non-default VRF.**
A.B.C.D	Enter the IPv4 address of the neighbor in dotted decimal format.
X:X:X:X::X	(OPTIONAL) Enter an IPv6 address.
peer-group *peer-group-name*	Enter the keywords `peer-group` then the name of the peer group to debug.
in	(OPTIONAL) Enter the keyword `in` to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword `out` to view only information on outbound BGP routes.
A.B.C.D	Enter the IP address of peer in the A.B.C.D format.
X:X:X:X::X	Enter the IPv6 IP address of peer in the X:X:X:X::X format.
dampening	Enter the keyword `dampening` to view BGP dampening.
events	Enter the keyword `events` to view BGP protocol events.
ipv4	Enter the ipv4 IP address to view the IPV4 route information.
ipv6	Enter the ipv6 IP address to view the IPV6 route information.
keepalives	Enter the keyword `keepalives` to view BGP keepalives.
notifications	Enter the keyword `notifications` to view BGP notifications.
soft-reconfiguration	Enter the keywords `soft-reconfiguration` to view only information on inbound BGP soft reconfiguration.
updates	Enter the keyword `updates` to view BGP updates.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

To view information on both incoming and outgoing routes, do not include the `in` and `out` parameters in the debugging command. The `in` and `out` parameters cancel each other; for example, if you enter the `debug ip bgp in` command and then enter the `debug ip bgp out` command, you do not see information on the incoming routes.

Entering a `no debug ip bgp` command removes all configured debug commands for BGP.

Related Commands

debug ip bgp events — views information about BGP events.

debug ip bgp keepalives — views information about BGP keepalives.

debug ip bgp notifications — views information about BGP notifications.

debug ip bgp updates — views information about BGP updates.

show debugging — views enabled debugging operations.

debug ip bgp dampening

View information on routes being dampened.

C9000 Series

Syntax

```
debug ip bgp [vrf vrf-name] [ipv4 {unicast | multicast} | ipv6 unicast]
dampening
```

To disable debugging, use the `no debug ip bgp dampening` command.

Parameters

vrf *vrf-name*	Enter the keyword `vrf` followed by the name of the VRF to view information on dampened routes corresponding to that VRF.

ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view dampened-route information related only to ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view dampened-route information related only to ipv4 unicast routes.
ipv6 *unicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view dampened-route information related only to ipv6 unicast routes.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

b

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced IPv6 MGBP support for the E-Series.

debug ip bgp events

Display information on local BGP state changes and other BGP events.

C9000 Series

Syntax `debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name] events [in | out]`

To disable debugging, use the `no debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name] events [in | out]` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to display BGP state changes corresponding to that VRF.
A.B.C.D	(OPTIONAL) Enter the IPv4 address of the neighbor.
X:X:X:X::X	(OPTIONAL) Enter an IPv6 address.

peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` then the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only events on inbound BGP messages.
out	(OPTIONAL) Enter the keyword `out` to view only events on outbound BGP messages.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

debug ip bgp keepalives

Display information about BGP keepalive messages.

C9000 Series

Syntax `debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name] keepalives [in | out]`

To disable debugging, use the `no debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name] keepalives [in | out]` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to display BGP keepalive information corresponding to that VRF.
A.B.C.D	(OPTIONAL) Enter the IPv4 address of the neighbor.
X:X:X:X::X	(OPTIONAL) Enter an IPv6 address.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` then the name of the peer group.

in	(OPTIONAL) Enter the keyword `in` to view only inbound keepalive messages.
out	(OPTIONAL) Enter the keyword `out` to view only outbound keepalive messages.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

debug ip bgp notifications

View information about BGP notifications received from neighbors.

C9000 Series

Syntax

```
debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name]
notifications [in | out]
```

To disable debugging, use the `no debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name] notifications [in | out]` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view neighbor BGP notification information corresponding to that VRF.
A.B.C.D	(OPTIONAL) Enter the IPv4 address of the neighbor.
X:X:X:X::X	(OPTIONAL) Enter an IPv6 address.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` then the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view BGP notifications received from neighbors.

	out	(OPTIONAL) Enter the keyword `out` to view BGP notifications sent to neighbors

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added ipv6 support.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

debug ip bgp soft-reconfiguration

Enable soft-reconfiguration debug.

C9000 Series

Syntax `debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group-name] soft-reconfiguration`

To disable, use the `debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group-name] soft-reconfiguration` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword vrf followed by the name of the VRF to enable soft-reconfiguration debugging on that VRF.
A.B.C.D	(OPTIONAL) Enter the IPv4 address of the neighbor in dotted decimal format.
X:X:X:X::X	(OPTIONAL) Enter an IPv6 address.
peer-group-name	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group..

Defaults Disabled

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.2.1.0	Introduced.

Usage Information

This command turns on BGP soft-reconfiguration inbound debugging. If no neighbor is specified, debug turns on for all neighbors.

debug ip bgp updates

View information about BGP updates.

C9000 Series

Syntax

`debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name] updates [in | out | prefix-list prefix-list-name]`

To disable debugging, use the `no debug ip bgp [vrf vrf-name] [A.B.C.D | X:X:X:X::X | peer-group peer-group-name] updates [in | out | prefix-list prefix-list-name]` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword vrf followed by the name of the VRF to view BGP updates information corresponding to that VRF.
A.B.C.D	(OPTIONAL) Enter an IPv4 address of the neighbor.
X:X:X:X::X	(OPTIONAL) Enter an IPv6 address.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

prefix-list *prefix-list-name*	(OPTIONAL) Enter the keyword `prefix-list` then the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group to disable or enable all routers within the peer group.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To remove all configured debug commands for BGP, enter the `no debug ip bgp` command.

default-metric

Allows you to change the metric of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

C9000 Series

Syntax `default-metric` *number*

To return to the default setting, use the `no default-metric` command.

Parameters

number	Enter a number as the metric to be assigned to routes from other protocols. The range is from 1 to 4294967295.

Defaults **0**

Command Modes ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The `default-metric` command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands

bgp always-compare-med — enables comparison of all BGP MED attributes.

redistribute — redistributes routes from other routing protocols into BGP.

deny bandwidth

Specify link bandwidth extended-community attribute as the matching criteria to deny incoming or outgoing traffic.

Syntax

```
deny bandwidth
```

To disable this setting, enter the `no deny bandwidth` command.

Parameters

bandwidth	Enter the keyword `bandwidth` to specify extended-community attribute as the matching criteria for denying traffic. The range is from 0 to 102400.

Defaults

N/A

Command Modes

EXTENDED COMMUNITY LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S-Series.

Related Commands

permit bandwidth – specify link band width extended-community attribute as the matching criteria to permitting incoming or outgoing traffic..

description

Enter a description of the BGP routing protocol

C9000 Series

Syntax

`description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the BGP protocol (80 characters maximum).

Defaults

none

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Related Commands

router bgp — enters ROUTER mode on the switch.

distance bgp

Define an administrative distance for routes.

C9000 Series

Syntax

`distance bgp external-distance internal-distance local-distance`

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is from 1 to 255. The default is **20**.

internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the network command. The range is from 1 to 255. The default is **200**.

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes ROUTER BGP (conf-router_bgp_af)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced IPv6 MGBP on the E-Series.

Usage Information

CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

C9000 Series

Syntax `maximum-paths {ebgp | ibgp} number`

To return to the default values, enter the `no maximum-paths` command.

Parameters

ebgp	Enter the keyword `ebgp` to enable multipath support for External BGP routes.

	ibgp	Enter the keyword `ibgp` to enable multipath support for Internal BGP routes.
	number	Enter a number as the maximum number of parallel paths. The range is from 2 to 64.

Defaults none

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Support from 2 to 64 paths on the S4810. Command syntax changed to `max-path` (was maximum-paths).
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information If you enable this command, use the `clear ip bgp *` command to recompute the best path.

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI (Address Family Identifier/Subsequent Address Family Identifier).

C9000 Series

Syntax `neighbor [ip-address | peer-group-name] activate`

To disable, use the `no neighbor [ip-address | peer-group-name] activate` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
activate	Enter the keyword `activate` to enable the neighbor/peer group in the new AFI/SAFI.

Defaults Disabled

Command Modes CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

By default, when you create a neighbor/peer group configuration in the Router BGP context, this enables IPv4/ Unicast AFI/SAFI. When you use `activate` in the new context, the neighbor/peer group enables for AFI/SAFI.

neighbor add-path

This command allows the specified neighbor/peer group to send/receive multiple path advertisements.

C9000 Series

Syntax

`neighbor [`*`ip-address`* `|` *`peer-group-name`*`] add-path [send | receive | both]` *`path-count`*

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	(OPTIONAL) Enter the name of the peer group.
send	Enter the keyword `send` to indicate that the system sends multiple paths to peers.
receive	Enter the keyword `receive` to indicate that the system accepts multiple paths from peers.
both	Enter the keyword `both` to indicate that the system sends and accepts multiple paths from peers.
path-count	Enter the number paths supported. The range is from 2 to 64.

Defaults

none

Command Modes

CONFIGURATION-ROUTER-BGP-ADDRESS FAMILY

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Inroduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Related Commands bgp add-path — allows the advertisement of multiple paths for the same address prefix without the new paths implicitly replacing any previous ones.

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

C9000 Series

Syntax

```
neighbor {ip-address | peer-group-name} advertisement-interval seconds
```

To return to the default value, use the `no neighbor {ip-address | peer-group-name} advertisement-interval` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. The range is from 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

Defaults

- seconds = **5 seconds** (internal peers)
- seconds = **30 seconds** (external peers)

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

neighbor advertisement-start

To send BGP routing updates, set the minimum interval before starting.

C9000 Series

Syntax

`neighbor {ip-address} advertisement-start seconds`

To return to the default value, use the `no neighbor {ip-address} advertisement-start` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
seconds	Enter a number as the time interval, in seconds, before BGP route updates are sent. The range is from 0 to 3600 seconds.

Defaults

none

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} allowas-in number`

To return to the default value, use the `no neighbor {ip-address | peer-group-name} allowas-in` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
number	Enter a number of times to allow this neighbor ID to use the AS path. The range is from 1 to 10.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Related Commands bgp four-octet-as-support — enables 4-byte support for the BGP process.

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

C9000 Series

Syntax `neighbor {ip-address | peer-group-name} default-originate [route-map map-name]`

To remove a default route, use the `no neighbor {ip-address | peer-group-name} default-originate` command.

Parameters

ip-address	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the default route of all routers in that peer group.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` then the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

C9000 Series

Syntax `neighbor {ip-address | peer-group-name} description text`

To delete a description, use the `no neighbor {ip-address | peer-group-name} description` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
text	Enter a continuous text string up to 80 characters.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

neighbor distribute-list

Distribute BGP information via an established prefix list.

C9000 Series

Syntax

`neighbor {`*`ip-address`* `|` *`peer-group-name`*`} distribute-list` *`prefix-list-name`* `{in | out}`

To delete a neighbor distribution list, use the `no neighbor {`*`ip-address`* `|` *`peer-group-name`*`} distribute-list` *`prefix-list-name`* `{in | out}` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.
prefix-list-name	Enter the name of an established prefix list. If the prefix list is not configured, the default is **permit** (to allow all routes).
in	Enter the keyword `in` to distribute only inbound traffic.
out	Enter the keyword `out` to distribute only outbound traffic.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information Other BGP filtering commands include: `neighbor filter-list`, `ip as-path access-list`, and `neighbor route-map`.

Related Commands ip as-path access-list — configures IP AS-Path ACL.

neighbor filter-list — assigns a AS-PATH list to a neighbor or peer group.

neighbor route-map — assigns a route map to a neighbor or peer group.

neighbor dmzlink-bw

Attach a Link Bandwidth to received routes.

C9000 Series

Syntax `neighbor {ip-address | peer-group} dmzlink-bw`

To disable BGP Link Bandwidth, enter the `no neighbor {ip-address | peer-group} dmzlink-bw` command.

Parameters

ip-address	Enter the IP address of the peer.
peer-group	Enter the name of the peer group.
dmzlink-bw	Enter the keyword `dmzlink-bw` to enable BGP Link Bandwidth in BGP multipath.

Defaults N/A

Command Modes ROUTER BGP

Command History

Version	Description
9.7(0.0)	Introduced on the S-Series and Z-Series.

Usage Information Configuring or un-configuring the command will bring down and bring up the BGP Route Manager, this will result in tear down and re-establishment of all active sessions.

Link Bandwidth has to be configured on the router in order to tell it to associate Link Bandwidth with prefixes (paths) and/or to use Link Bandwidth in BGP Multipath route selection.

This is done under BGP configuration and is supported per address family – for IPv4 and IPv6 address families.

The configuration for a particular address family will apply across all VRFs configured.

This command must be performed on the router which is attaching link bandwidth to prefixes (typically a border router) as well as the router which is expected to load share traffic proportional to the bandwidth of the external links.

neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} ebgp-multihop [ttl]`

To disallow and disconnect connections, use the `no neighbor {ip-address | peer-group-name} ebgp-multihop` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
ttl	(OPTIONAL) Enter the number of hops as the Time to Live (ttl) value. The range is from 1 to 255. The default is **255**.

Defaults

Disabled.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

To prevent loops, the `neighbor ebgp-multihop` command does not install the default routes of the multihop peer. Networks not directly connected are not considered valid for best-path selection.

neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

C9000 Series

Syntax

`neighbor {ipv4-address | peer-group-name} fall-over`

To disable, use the `no neighbor {ipv4-address | peer-group-name} fall-over` command.

Parameters

ipv4-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.

Defaults

Disabled.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.4.1.0	Introduced

Usage Information

When you enable failover, BGP keeps track of IP or IPv6 ability to reach the peer remote address and the peer local address. Whenever either address becomes unreachable (for example, no active route exists in the routing table for the peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands

show ip bgp neighbors — displays information on the BGP neighbors.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} filter-list as-path-name {in | out}`

To delete a BGP filter, use the `no neighbor {ip-address | peer-group-name} filter-list as-path-name {in | out}` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
as-path-name	Enter the name of an established AS-PATH access list (up to 140 characters). If the AS-PATH access list is not configured, the default is **permit** (allow routes).
in	Enter the keyword `in` to filter inbound BGP routes.
out	Enter the keyword `out` to filter outbound BGP routes.

Defaults

Not configured.

Command Modes

- ROUTER BGP
- ROUTER BGP-address-family

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series. Increased the name string to accept up to 140 characters. Prior to 7.8.1.0, ACL names were up to 16 characters long.
7.7.1.0	Introduced on the C-Series.

Usage Information

To enter AS-PATH ACL mode and configure the AS-PATH filters to deny or permit BGP routes based on information in their AS-PATH attribute, use the `ip as-path access-list` command in CONFIGURATION mode.

Related Commands

ip as-path access-list — enter AS-PATH ACL mode and configure the AS-PATH filters.

neighbor local-as

To accept external routes from neighbors with a local AS number in the AS number path, configure Internal BGP (IBGP) routers.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} local-as as-number [no-prepend]`

To return to the default value, use the `no neighbor {ip-address | peer-group-name} local-as` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
as-number	Enter the AS number to reset all neighbors belonging to that AS. The range is from 0 to 65535 (2 byte), from 1 to 4294967295 (4 byte) or from 0.1 to 65535.65535 (dotted format).
no prepend	Specifies that local AS values do not prepend to announcements from the neighbor.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Related Commands

bgp four-octet-as-support — enables 4-byte support for the BGP process.

neighbor maximum-prefix

Control the number of network prefixes received.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]`

To return to the default values, use the `no neighbor {ip-address | peer-group-name} maximum-prefix maximum` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the E-Series software sends a message. The range is from 1 to 100 percent. The default is **75**.
warning-only	(OPTIONAL) Enter the keyword `warning-only` to set the router to send a log message when the maximum value is reached. If this parameter is not set, the router stops peering when the maximum number of prefixes is reached.

Defaults

threshold = **75**

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

If you configure the `neighbor maximum-prefix` command and the neighbor receives more prefixes than the `neighbor maximum-prefix` command configuration allows, the neighbor goes down and the `show ip bgp summary` command displays (prfxd) in the State/PfxRcd column for that neighbor. The neighbor remains down

until you enter the `clear ip bgp` command for the neighbor or the peer group to which the neighbor belongs or you enter the `neighbor shutdown` and `neighbor no shutdown` commands.

Related Commands show ip bgp summary — displays the current BGP configuration.

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

C9000 Series

Syntax

`neighbor {ipv6-address | peer-group-name} next-hop-self [all]`

To return to the default setting, use the `no neighbor {ipv6-address | peer-group-name} next-hop-self [all]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	(OPTIONAL) Enter the name of the peer group.
all	Specifies that the route reflector is the next hop for both iBGP and eBGP-learned routes.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.10(0.0)	Introduced the `all` keyword on the S4810, S4820, S4048–ON, S3048–ON, S3100 series, S6010–ON, S4040T-ON, S5000, S6000, S6000–ON, S6100–ON, Z9100–ON, and Z9500.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

If you configure the `set ipv6 next-hop` command in ROUTE-MAP mode, its configuration takes precedence over the `neighbor next-hop-self` command.

If you do not use the `all` keyword, the next hop of only eBGP-learned routes is updated by the route reflector. If you use the `all` keyword, the next hop of both eBGP- and iBGP-learned routes are updated by the route reflector.

neighbor password

Enable message digest 5 (MD5) authentication on the TCP connection between two neighbors.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} password [encryption-type] password`

To delete a password, use the `no neighbor {ip-address | peer-group-name} password` command.

Parameters

ip-address	Enter the IP address of the router to be included in the peer group.
peer-group-name	Enter the name of a configured peer group.
encryption-type	(OPTIONAL) Enter `7` as the encryption type for the password entered. `7` means that the password is encrypted and hidden.
password	Enter a text string up to 80 characters long. The first character of the password must be a letter. You cannot use spaces in the password.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

Configure the same password on both BGP peers or a connection does not occur. When you configure MD5 authentication between two BGP peers, each segment of the TCP connection between them is verified and the MD5 digest is checked on every segment sent on the TCP connection.

Configuring a password for a neighbor causes an existing session to be torn down and a new one established.

If you specify a BGP peer group by using the `peer-group-name` parameter, all the members of the peer group inherit the characteristic configured with this command.

If you configure a password on one neighbor, but you have not configured a password for the neighboring router, the following message appears on the console while the routers attempt to establish a BGP session between them:

```
%RPM0-P:RP1 %KERN-6-INT: No BGP MD5 from [peer's IP address]
:179 to [local router's IP address]:65524
```

Also, if you configure different passwords on the two routers, the following message appears on the console:

```
%RPM0-P:RP1 %KERN-6-INT: BGP MD5 password mismatch from
[peer's IP address] : 11502 to [local router's IP address] :179
```

neighbor peer-group (assigning peers)

Allows you to assign one peer to an existing peer group.

C9000 Series

Syntax

`neighbor` *ip-address* `peer-group` *peer-group-name*

To delete a peer from a peer group, use the `no neighbor` *ip-address* `peer-group` *peer-group-name* command.

Parameters

ip-address	Enter the IP address of the router to be included in the peer group.
peer-group-name	Enter the name of a configured peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

You can assign up to 256 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- neighbor advertisement-interval

- neighbor distribute-list
- neighbor filter-list
- neighbor route-map
- neighbor route-reflector-client
- neighbor send-community

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's, and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown) the peers within the group are also disabled (shutdown).

Related Commands

clear ip bgp — resets BGP sessions.

neighbor peer-group (creating group) — creates a peer group.

show ip bgp peer-group — views BGP peers.

show ip bgp neighbors — views BGP neighbors configurations.

neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

C9000 Series

Syntax

`neighbor` *`peer-group-name`* `peer-group`

To delete a peer group, use the `no neighbor` *`peer-group-name`* `peer-group` command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Version	Description
7.7.1.0	Introduced on the C-Series.

Usage Information When you create a peer group, it is disabled (Shut mode).

Related Commands neighbor peer-group (assigning peers) — assigns routers to a peer group.

neighbor remote-as — assigns a indirectly connected AS to a neighbor or peer group.

neighbor shutdown — disables a peer or peer group.

neighbor peer-group passive

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but responds to one.

C9000 Series

Syntax `neighbor peer-group-name peer-group passive [sessions]`

To delete a passive peer-group, use the `no neighbor peer-group-name peer-group passive` command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced the `limit` keyword on the S4810.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information After you configure a peer group as passive, assign it a subnet using the `neighbor soft-reconfiguration inbound` command.

For passive eBGP limits, the Remote AS must be different from the AS for this neighbor.

Related Commands

neighbor soft-reconfiguration inbound — assigns a subnet to a dynamically configured BGP neighbor.

neighbor remote-as — assigns an indirectly connected AS to a neighbor or peer group.

neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} remote-as number`

To delete a remote AS entry, use the `no neighbor {ip-address | peer-group-name} remote-as number` command.

Parameters

ip-address	Enter the IP address of the neighbor to enter the remote AS in its routing table.
peer-group-name	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
number	Enter a number of the AS. The range is from 0 to 65535 (2 byte) or from 1 to 4294967295 (4 byte).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series. Added 4-byte support.

Usage Information

To accept 4-byte formats before entering a 4 byte AS Number, configure your system. If the `number` parameter is the same as the AS number used in the `router bgp` command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (Shutdown).

Related Commands

router bgp — enters ROUTER BGP mode and configures routes in an AS.

bgp four-octet-as-support — enables 4-byte support for the BGP process.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} remove-private-as`

To return to the default, use the `no neighbor {ip-address | peer-group-name} remove-private-as` command.

Parameters

ip-address	Enter the IP address of the neighbor to remove the private AS numbers.
peer-group-name	Enter the name of the peer group to remove the private AS numbers.

Defaults

Disabled (that is, private AS number are not removed).

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series. Added 4-byte support.

Usage Information

Applies to EBGP neighbors only.

Configure your system to accept 4-byte formats before entering a 4 byte AS Number.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are from 64512 to 65535 (2 byte).

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} route-map map-name {in | out}`

To remove the route map, use the `no neighbor {ip-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If the Route map is not configured, the default is **deny** (to drop all routes).
in	Enter the keyword `in` to filter inbound routes.
out	Enter the keyword `out` to filter outbound routes.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure the router as a route reflector and the specified neighbors as members of the cluster.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} route-reflector-client`

To remove one or more neighbors from a cluster, use the `no neighbor {ip-address | peer-group-name} route-reflector-client` command. If you delete all members of a cluster, you also delete the route-reflector configuration on the router.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

A route reflector reflects routes to the neighbors assigned to the cluster. Neighbors in the cluster do not need not to be fully meshed. By default, when you use `no route reflector`, the internal BGP (IBGP) speakers in the network must be fully meshed.

The first time you enter this command, the router configures as a route reflector and the specified BGP neighbors configure as clients in the route-reflector cluster.

When you remove all clients of a route reflector using the `no neighbor route-reflector-client` command, the router no longer functions as a route reflector.

If the clients of a route reflector are fully meshed, you can configure the route reflector to not reflect routes to specified clients by using the `no bgp client-to-client reflection` command.

Related Commands bgp client-to-client reflection — enables route reflection between the route reflector and the clients.

neighbor send-community

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

C9000 Series

Syntax `neighbor {ip-address | peer-group-name} send-community`

To disable sending a COMMUNITY attribute, use the `no neighbor {ip-address | peer-group-name} send-community` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.
extended	Optional. Enter the keyword `extended` to send extended community attribute.
standard	Optional. Enter the keyword `standard` to send standard community attribute.

Defaults Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information To configure a COMMUNITY attribute, use the `set community` command in ROUTE-MAP mode.

Before using this command, you must execute the `clear ip bgp` command.

neighbor shutdown

Disable a BGP neighbor or peer group.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} shutdown`

To enable a disabled neighbor or peer group, use the `neighbor {ip-address | peer-group-name} no shutdown` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults

Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

Peers that are enabled within a peer group are disabled when their peer group is disabled.

The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shut down, use the `show ip bgp summary` command to confirm its status.

Related Commands

show ip bgp summary — displays the current BGP configuration.

show ip bgp neighbors — displays the current BGP neighbors.

neighbor soft-reconfiguration inbound

Enable soft-reconfiguration for BGP.

C9000 Series

Syntax

```
neighbor {ip-address | peer-group-name} soft-reconfiguration inbound
```

To disable, use the `no neighbor {ip-address | peer-group-name} soft-reconfiguration inbound` command.

Parameters

ip-address	Enter the IP address of the neighbor in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults Disabled

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

Usage Information This command enables soft-reconfiguration for the BGP neighbor specified. BGP stores all the updates the neighbor receives but does not reset the peer-session.

CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.

NOTE: This command is supported in BGP Router Configuration mode for IPv4 Unicast address only.

Related Commands show ip bgp neighbors — displays routes received by a neighbor.

neighbor subnet

Enable passive peering so that the members of the peer group are dynamic.

C9000 Series

Syntax

`neighbor` *peer-group-name* `subnet` *subnet-number mask*

To remove passive peering, use the `no neighbor` *peer-group-name* `subnet` *subnet-number mask* command.

Parameters

subnet-number	Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the Peer group. To allow all addresses, enter `0.0.0.0/0`.
mask	Enter a prefix mask in / prefix-length format (/x).

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

C9000 Series

Syntax

`neighbor {`*ip-address* | *peer-group-name*`} timers` *keepalive holdtime*

To return to the default values, use the `no neighbor {`*ip-address* | *peer-group-name*`} timers` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is from 1 to 65535. The default is **60 seconds**.
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is **180 seconds**.

Defaults

- keepalive = **60 seconds**
- holdtime = **180 seconds**

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information Timer values configured with the `neighbor timers` command override the timer values configured with any other command.

When two neighbors, configured with different `keepalive` and `holdtime` values, negotiate for new values, the resulting values are as follows:

- the lower of the `holdtime` value is the new `holdtime` value, and
- whichever is the lower value; one-third of the new `holdtime` value, or the configured `keepalive` value, is the new keepalive value.

neighbor timers extended

Set idle hold time for a BGP neighbor or a peer group.

Syntax `neighbor {`*`ip-address`* `|` *`ipv6-address`* `|` *`peer-group-name`*`} timers extended` *`idle holdtime`*

To return to the default values, use the `no neighbor {`*`ip-address`* `|` *`ipv6-address`* `|` *`peer-group-name`*`} timers extended` *`idle holdtime`* command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
ipv6-address	Enter the IPv6 address of the peer router in X:X:X:X::X format.
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
timers extended *idle holdtime*	Enter a number for the time interval, in seconds, for the peer to be idle state. The range is from 1 to 32767. The default is **15 seconds**.

Defaults The default idle holdtime is **15 seconds**.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the C9010, MXL, FN IOM, S3100 series, S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000, S6010–ON, S6100–ON, Z9100–ON, and S6000–ON.

Usage Information The peer remains in idle state based on the configured `idle holdtime`. The less the `idle holdtime`, less the peer in idle state.

For the new *idle holdtime* to take effect, you need to shutdown the respective peer manually using `neighbor shutdown` command and enable the peer again.

neighbor update-source

Enable the system to use Loopback interfaces for TCP connections for BGP sessions.

C9000 Series

Syntax `neighbor {ip-address | peer-group-name} update-source interface`

To use the closest interface, use the `no neighbor {ip-address | peer-group-name} update-source interface` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
interface	Enter the keyword `loopback` then a number of the Loopback interface. The range is from 0 to 16383.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced ont he C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

C9000 Series

Syntax `neighbor {ip-address | peer-group-name} weight weight`

To remove a weight value, use the `no neighbor {ip-address | peer-group-name} weight` command.

Parameters

ip-address	Enter the IP address of the peer router in dotted decimal format.
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
weight	Enter a number as the weight. The range is from 0 to 65535. The default is **0**.

Defaults **0**

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

In the best path selection process, the path with the highest weight value is preferred.

NOTE: In the best-path selection process, the path with the highest weight value is preferred.

If you configure the `set weight` command in a route map applied to this neighbor, the weight set in that command overrides the weight set in the `neighbor weight` command.

Related Commands

set weight — assigns a weight to all paths meeting the route map criteria.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

C9000 Series

Syntax

`network ip-address mask [route-map map-name]`

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` then the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is **deny** (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

Dell Networking OS software resolves the network address the `network` command configures with the routes in the main routing table to ensure that the networks are reachable using non-BGP routes and non-default routes.

As BGP does not query next-hop information corresponding to locally originated routes, a local route with an unreachable next-hop is chosen as the best route.

When a combination of locally originated and peer originated routes occurs, both these routes will exist in the RTM. However, only the best route is kept active in the RTM and the remaining route is rendered in-active.

It is possible to keep only one locally originated route in the BGP database. Network command has preference over the re-distributed routes. When the locally originated route is no longer present in the database the other route is automatically installed.

In BGP, the next-hop for the route is calculated from the information that is acquired through IGP or static routes.

Related Commands

redistribute — redistributes routes into BGP.

network backdoor

Specify this IGP route as the preferred route.

C9000 Series

Syntax

`network` *`ip-address mask`* `backdoor`

To remove a network, use the `no network` *`ip-address mask`* `backdoor` command.

Parameters

ip-address	Enter an IP address in dotted decimal format of the network.
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).

Defaults

Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information Although the system does not generate a route due to the backdoor config, there is an option for injecting/ sourcing a local route in the presence of network backdoor config on a learned route.

permit bandwidth

Specify link bandwidth extended-community attribute as the matching criteria to permit incoming or outgoing traffic.

Syntax `permit bandwidth`

To disable this setting, enter the `no permit bandwidth` command.

Parameters

bandwidth	Enter the keyword `bandwidth` to specify extended-community attribute as the matching criteria for permitting traffic. The range is from 0 to 102400.

Defaults N/A

Command Modes EXTENDED COMMUNITY LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S-Series.

Related Commands deny bandwidth – link bandwidth extended-community attribute as the matching criteria to deny incoming or outgoing traffic..

redistribute

Redistribute routes into BGP.

C9000 Series

Syntax

`redistribute {connected | static} [route-map map-name]`

To disable redistribution, use the `no redistribution {connected | static}` command.

Parameters

connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keyword `route-map` then the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ip address • set community • set local-preference • set metric • set next-hop • set origin • set weight If the route map is not configured, the default is **deny** (to drop all routes).

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the ability to substitute IGP cost for MED when a peer/peer-group outbound route-map is set as **internal**.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

You can use the `redistribute` command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and applied outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-groups have the IGP cost set as **MED**.

If you do not configure the `default-metric` command, in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is "0".

To redistribute the default route (0.0.0.0/0), configure the `neighbor default-originate` command.

As BGP does not query next-hop information corresponding to locally originated routes, a local route with an unreachable next-hop is chosen as the best route.

When a combination of locally originated and peer originated routes occurs, both these routes will exist in the RTM. However, only the best route is kept active in the RTM and the remaining route is rendered in-active.

It is possible to keep only one locally originated route in the BGP database. Network command has preference over the re-distributed routes. When the locally originated route is no longer present in the database the other route is automatically installed.

Related Commands

neighbor default-originate — injects the default route.

redistribute ospf

Redistribute OSPF routes into BGP.

C9000 Series

Syntax

`redistribute ospf` *`process-id`* `[[match external {1 | 2}] [match internal]] [route-map` *`map-name`*`]`

To stop redistribution of OSPF routes, use the `no redistribute ospf` *`process-id`* command.

Parameters

process-id	Enter the number of the OSPF process. The range is from 1 to 65535.
match external {1 | 2}	(OPTIONAL) Enter the keywords `match external` to redistribute OSPF external routes. You can specify `1` or `2` to redistribute those routes only.
match internal	(OPTIONAL) Enter the keywords `match internal` to redistribute OSPF internal routes only.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the ability to substitute IGP cost for MED when a peer/peer-group outbound route-map is set as **internal**.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information You can use the `redistribute` command to advertise the IGP cost as the MED on redistributed routes. When you set the route-map with metric-type internal and apply outbound to an EBGP peer/peer-group, the advertised routes corresponding to those peer/peer-groups have the IGP cost set as **MED**.

When you enter the `redistribute isis` *`process-id`* command without any other parameters, the system redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes. RFC does not support this feature.

router bgp

To configure and enable BGP, enter ROUTER BGP mode.

Syntax `router bgp` *`as-number`*

To disable BGP, use the `no router bgp` *`as-number`* command.

Parameters

as-number	Enter the AS number. The range is from 1 to 65535 (2 byte), from 1 to 4294967295 (4 byte), or from 0.1 to 65535.65535 (dotted format).

Defaults Not enabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.

Version	Description
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000–ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

At least one interface must be in Layer 3 mode for the `router bgp` command to be accepted. If all interfaces are configured under VRF, at least one interface should be in the default VRF for the `router bgp` command to be accepted. If no interfaces are enabled for Layer 3, an error message appears:

```
% Error: No router id
configured
```

BGP does not allow 23456 (AS-TRANS) as a configured AS number.

Example

```
DellEMC(conf)# router bgp 3
DellEMC(conf-router_bgp)#
```

set extcommunity bandwidth

Set extended community bandwidth for handling inbound and outbound policies.

Syntax

`set extcommunity bandwidth`

To disable extended community bandwidth, enter the `no set extcommunity bandwidth` command.

Parameters

bandwidth	Enter the keyword `bandwidth` to enable extended community bandwidth. The range is from 0 to 102400.

Defaults

N/A

Command Modes

ROUTER MAP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S-Series.

Usage Information

A new policy command is introduced in order to attach the Link Bandwidth extended community only to the prefixes that are received from a neighbor that satisfy the desired conditions. This command is relevant for both inbound as well as outbound policy handling (for received prefixes). Also, there is no change to the set of supported conditions or filters.

During configuration, the bandwidth is specified in Mbps, not in bytes/second. While creating the actual LB extended community, the system will attach the AS number and encode the bandwidth in floating point format.

shutdown all

Disables all the BGP neighbors.

Syntax

```
shutdown all
```

Use the `no shutdown all` command to enable all the configured BGP neighbors.

Command Modes

ROUTER BGP

Command History

Version	Description
9.11.0.0	Introduced on the S-Series, Z-Series, MXL, and IOM.

Usage Information

You can use this command to disable all the configured BGP neighbors.

This command is global for all VRFs.

shutdown address-family-ipv4–multicast

Disables all the BGP neighbors corresponding to the multicast IPv4 address families.

Syntax

```
shutdown address-family-ipv4-unicast
```

Use the `no shutdown address-family-ipv4-unicast` command to enable all the configured BGP neighbors corresponding to the multicast IPv4 address families.

Command Modes

ROUTER BGP

CONFIGURATION

Command History

Version	Description
9.11.0.0	Introduced on the S-Series, Z-Series, MXL, and IOM.

Usage Information

You can use this command to disable all the configured BGP neighbors corresponding to the multicast IPv4 address families.

This command is global for all VRFs.

shutdown address-family-ipv4–unicast

Disables all the BGP neighbors corresponding to the unicast IPv4 address families.

Syntax

`shutdown address-family-ipv4-unicast`

Use the `no shutdown address-family-ipv4-unicast` command to enable all the configured BGP neighbors corresponding to the unicast IPv4 address families.

Command Modes

ROUTER BGP

CONFIGURATION

Command History

Version	Description
9.11.0.0	Introduced on the S-Series, Z-Series, MXL, and IOM.

Usage Information

You can use this command to disable all the configured BGP neighbors corresponding to the unicast IPv4 address families.

This command is global for all VRFs.

shutdown address-family-ipv6–unicast

Disables all the BGP neighbors corresponding to the unicast IPv6 address families.

Syntax

`shutdown address-family-ipv6-unicast`

Use the `no shutdown address-family-ipv6-unicast` command to enable all the configured BGP neighbors corresponding to the unicast IPv6 address families.

Command Modes

ROUTER BGP

CONFIGURATION

Command History

Version	Description
9.11.0.0	Introduced on the S-Series, Z-Series, MXL, and IOM.

Usage Information

You can use this command to disable all the configured BGP neighbors corresponding to the unicast IPv6 address families.

This command is global for all VRFs.

show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv4 address on the system.

C9000 Series

Syntax `show capture bgp-pdu neighbor ipv4-address`

Parameters

ipv4-address	Enter the IPv4 address (in dotted decimal format) of the BGP address to display packet information for that address.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced.

Example

```
Dell(conf-router_bgp)#show capture bgp-pdu neighbor 20.20.20.2

Incoming packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 26 packet(s) captured using 680 bytes
  PDU[1] : len 101, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00650100 00000013 00000000
00000000 419ef06c 00000000
    00000000 00000000 00000000 00000000 0181a1e4 0181a25c 41af92c0
00000000 00000000 00000000
    00000000 00000001 0181a1e4 0181a25c 41af9400 00000000
  PDU[2] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
  PDU[3] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
 [. . .]

Outgoing packet capture enabled for BGP neighbor 20.20.20.2
Available buffer size 40958758, 27 packet(s) captured using 562 bytes
  PDU[1] : len 41, captured 00:34:52 ago
    ffffffff ffffffff ffffffff ffffffff 00290104 000100b4 14141401
0c020a01 04000100 01020080
    00000000
  PDU[2] : len 19, captured 00:34:51 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
```

```
  PDU[3] : len 19, captured 00:34:50 ago
    ffffffff ffffffff ffffffff ffffffff 00130400
 [. . .]
Dell#
```

Related Commands capture bgp-pdu max-buffer-size — specifies a size for the capture buffer.

show config

View the current ROUTER BGP configuration.

C9000 Series

Syntax `show config`

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Example

```
Dell(conf-router_bgp)#show config
!
router bgp 45
 neighbor suzanne peer-group
 neighbor suzanne no shutdown
 neighbor sara peer-group
 neighbor sara shutdown
 neighbor 13.14.15.20 peer-group suzanne
 neighbor 13.14.15.20 shutdown
 neighbor 123.34.55.123 peer-group suzanne
 neighbor 123.34.55.123 shutdown
Dell(conf-router_bgp)#
```

Related Commands capture bgp-pdu max-buffer-size — specifies a size for the capture buffer.

show ip bgp

View the current BGP IPv4 routing table for the system.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {unicast | multicast} | ipv6 {unicast}]
[network [network-mask] [longer-prefixes]] [cluster-list cluster-id] [community
community-number] [community-list community-list-name] [dampened-paths]
[extcommunity-list list name] [filter-list as-path-name] [flap-statistics [ip-
address [mask]]] [neighbors [all {received-routes}] [network[network-mask]]]
[next-hop] [paths] [peer-group peer-group-name] [regexp regular-expression]
[summary]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view ipv4–unicast route information corresponding to that VRF.
ipv4 unicast	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
ipv4 multicast	(OPTIONAL) Enter the keywords `ipv4 multicast` to view information only related to ipv4 multicast routes.
ipv6 unicast	(OPTIONAL) Enter the keywords `ipv6 unicast` to view information only related to ipv6 unicast routes.
network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.
cluster-list *cluster-id*	(OPTIONAL) Enter the keyword `cluster-list` then the *cluster-ID* to display the routes matching the cluster.
community *community-number*	(OPTIONAL) Enter the keyword `community` then the *community–number* to display the routes matching the communities.
community-list*community-list-name*	(OPTIONAL) Enter the keyword `community-list` then the *community–list–name* to display the routes matching the community–list
dampened-paths	(OPTIONAL) Enter the keyword `dampened-paths` to display the paths suppressed due to dampening.
extcommunity-list *list name*	(OPTIONAL) Enter the keyword `extcommunity-list` then the *list name* to display the routes matching the extended community-list.
filter-list *as-path-name*	(OPTIONAL) Enter the keyword `filter-list` then the *as-path-name* to display the routes conforming to the filter–list.
flap-statistics	(OPTIONAL) Enter the keyword `flap-statistics` to display flap statistics of the routes.
neighbors	(OPTIONAL) Enter the keyword `neighbors` to display the detailed information on TCP and BGP neighbor connections.

neighbors [all {received-routes}]	(OPTIONAL) Enter the keyword `neighbors [all {received-routes}]` to display all the received routes both accepted and rejected from all the IPv4 or IPv6 neighbors.
next-hop	(OPTIONAL) Enter the keyword `next-hop` to view all the next-hop information on the learnt routes.
paths	(OPTIONAL) Enter the keyword `paths` to view the BGP path attributes in the BGP database.
peer-group *peer-group-name*	(OPTIONAL) Enter the keyword `peer-group` then the `peer-group-name` to view the information on the BGP peers in a peer group.
regexp *regular-expression*	(OPTIONAL) Enter the keyword `regexp` then the *regular expressions* to display BGP information based on a regular expression.
summary	(OPTIONAL) Enter the keyword `summary` to display the summary of BGP neighbor status.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.14(0.0)	Introduced the `[all {received-routes}]` option for IPv4 and IPv6 neighbors.
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Added the `add-path` option to the S4810. Output on the S4810 shows the ADDPATH parameters.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

When you enable the `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

In BGP, this command displays the exact reason why the route is discarded.

The following describes the `show ip bgp` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.

Field	Description
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

The `show ip bgp` command displays the dmzlink-dw details only if dmzlink-bw is enabled using the `bgp dmzlink-dw` command.

Example

```
Dell EMC#show ip bgp
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>  55.0.0.0/24        172.16.0.2                               0 200 i
*>  66.0.0.0/24        172.16.0.2                               0 200 i
```

All the show and debugs commands display the link band width extended-community prefixed with DMZ-Link-bw along with other extended communities.

```
Dell EMC#show ip bgp 3.3.3.0/24
BGP routing table entry for 3.3.3.0/24
Paths: (1 available, table Default-IP-Routing-Table.)
Not advertised to any peer
Received from :
 1.1.1.2 (3.3.3.1)   Best
  AS_PATH :
  Next-Hop : 1.1.1.2, Cost : 0
  Origin IGP, Metric  0, LocalPref  100, Weight  0, internal
 Extended Communities :
  DMZ-Link Bw: 2000 kbytes*
```

Related Commands

show ip bgp community — views the BGP communities.

neighbor maximum-prefix — controls the number of network prefixes received.

show ip bgp cluster-list

View BGP neighbors in a specific cluster.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] cluster-
list [cluster-id]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view cluster information of BGP neighbors corresponding to that VRF.

ipv4 *multicast*	(OPTIONAL) Enter the keywords `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 multicast routes.
ipv6 *unicast*	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related to only to the ipv6 unicast routes.
cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format. The range is 1 — 4294967295.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp cluster-list` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#show ip bgp cluster-list
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.6
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
```

```
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>I 55.0.0.0/24        172.16.0.2                           0      0 400 500
600 i
*>I 66.0.0.0/24        172.16.0.2                           0      0 500 i
*>I 77.0.0.0/24        172.16.0.2                           0      0 i

Dell#show ip bgp cluster-list 4.4.4.4
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.6
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>I 55.0.0.0/24        172.16.0.2                           0      0 400 500
600 i
*>I 66.0.0.0/24        172.16.0.2                           0      0 500 i
*>I 77.0.0.0/24        172.16.0.2                           0      0 i
Dell#
```

show ip bgp community

View information on all routes with Community attributes or view specific BGP community groups.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast]
community [community-number] [local-as] [no-export] [no-advertise]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view information either on all routes with community attributes or specific BGP community routes corresponding to that VRF.
ipv4 *unicast*	(OPTIONAL) Enter the keywords `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
ipv6 *unicast*	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED.

All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.

no-advertise Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE.

All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.

no-export Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT.

All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

The following describes the `show ip bgp community` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.

Field	Description
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#show ip bgp community ?
local-AS                Do not export 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)
aa:nn                   Community number in aa:nn format
|                       Pipe through a command

Dell#show ip bgp community
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>  55.0.0.0/24        172.16.0.2                               0 200 i
*>  66.0.0.0/24        172.16.0.2                               0 200 i

Dell#show ip bgp community no-advertise
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>  66.0.0.0/24        172.16.0.2                               0 200 i
```

show ip bgp community-list

View routes that a specific community list affects.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {unicast | multicast} | ipv6 unicast]
community-list community-list-name [exact-match]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view routes affected by a specific community list corresponding to that VRF.
ipv4 *unicast*	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.

ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
ipv6 *unicast*	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
community-list-name	Enter the name of a configured IP community list (maximum 140 characters).
exact-match	Enter the keyword for an exact match of the communities.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The `show ip bgp community-list` command without any parameters lists BGP routes matching the Community List and the output is the same as for the `show ip bgp` command output.

The following describes the `show ip bgp community-list pass` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#conf t
Dell(conf)#ip community-list cl1
Dell(config-community-list)#permit 1000:1
Dell(config-community-list)#end
Dell#show ip bgp community-list cl1
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>  55.0.0.0/24        172.16.0.2                               0 200 i
Dell#show ip bgp 55.0.0.0/24
BGP routing table entry for 55.0.0.0/24
Paths: (1 available, table Default-IP-Routing-Table.)
Not advertised to any peer

Received from :
 172.16.0.2 (172.16.0.2)   Best
  AS_PATH : 200

  Next-Hop : 172.16.0.2, Cost : 0
  Origin IGP, Metric  4294967295 (Default), LocalPref  100, Weight  0, external


 Communities :
  200:1        1000:1       3000:1
```

show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast]
dampened-paths
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view routes that are affected by a specific community list corresponding to that VRF.
ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
ipv4 *unicast*	(OPTIONAL) Enter the keywords `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

To determine a BGP session flap, both a route-down event and a subsequent route-up event corresponding to a single route are considered. As a result, a flap event is penalized only one time during the route-down event. The subsequent route-up event corresponding to the same route is not considered as a flap and is not penalized.

The history paths that the `show ip bgp` command displays contain only the prefix and the next-hop information. The next-hop information shows the ip address of the neighbor. It does not show the actual next-hop details.

The following describes the `show ip bgp damp` command shown in the following example.

Field	Description
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

Example

```
Dell#show ip bgp dampened-paths
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            From            Reuse     Path

d   55.0.0.0/24      172.16.0.2             00:36:23      200

Dell#
```

show ip bgp detail

Display BGP internal information for the IPv4 Unicast address family.

C9000 Series

Syntax `show ip bgp [ipv4 unicast] detail`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced.

Example

```
Dell#show ip bgp detail
Detail information for BGP Node
bgpNdP 0x41a17000 : NdTmrP 0x41a17000 : NdKATmrP 0x41a17014 : NdTics 74857 :
NhLocAS 1 : NdState 2 : NdRPMPrim 1 : NdListSoc 13
NdAuto 1 : NdEqCost 1 : NdSync 0 : NdDefOrg 0
NdV6ListSoc 14 NdDefDid 0 : NdConfedId 0 : NdMedConfed 0 : NdMedMissVal -1 :
NdIgnrIllId 0 : NdRRC2C 1 : NdClstId 33686273 : NdPaTblP 0x41a19088
NdASPTblP 0x41a19090 : NdCommTblP 0x41a19098 : NhOptTransTblP 0x41a190a0 :
NdRRClsTblP 0x41a190a8
NdPktPA 0 : NdLocCBP 0x41a6f000 : NdTmpPAP 0x419efc80 : NdTmpASPAP 0x41a25000 :
NdTmpCommP 0x41a25800
NdTmpRRClP 0x41a4b000 : NdTmpOptP 0x41a4b800 : NdTmpNHP : NdOrigPAP 0
NdOrgNHP 0 : NdModPathP 0x419efcc0 : NdModASPAP 0x41a4c000 : NdModCommP
0x41a4c800
NdModOptP 0x41a4d000 : NdModNHP : NdComSortBufP 0x41a19110 : NdComSortHdP
0x41a19d04 : NdUpdAFMsk 0 : AFRstSet 0x41a1a298 : NHopDfrdHdP 0x41a1a3e0 :

NumNhDfrd 0 : CfgHdrAFMsk 1
AFChkNetTmrP 0x41ee705c : AFRtDamp 0 : AlwysCmpMed 0 : LocrHld 10 : LocrRem
10 :
softReconfig 0x41a1a58c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a0d100 : Starts 0 : Stops 0 : Opens 0
Closes 0 : Fails 0 : Fatals 0 : ConnExps 0 : HldExps 0 : KeepExps 0
RxOpens 0 : RxKeeps 0 : RxUpds 0 : RxNotifs 0 : TxUpds 0 : TxNotifs 0
```

```
BadEvts 0 : SynFails 0 : RxeCodeP 0x41a1b6b8 : RxHdrCodeP 0x41a1b6d4 :
RxOpCodeP
0x41a1b6e4
RxUpdCodeP 0x41a1b704 : TxEcodeP 0x41a1b734 : TxHdrcodeP 0x41a1b750 : TxOpCodeP
0x41a1b760
TxUpdCodeP 0x41a1b780 : TrEvt 0 : LocPref 100 : tmpPathP 0x41a1b7b8 :
LogNbrChgs 1
RecursiveNH 1 : PgCfgId 0 : KeepAlive 0 : HldTime 0 : DioHdl 0 : AggrValTmrP
0x41ee7024
UpdNetTmrP 0 : RedistTmrP 0x41ee7094 : PeerChgTmrP 0 : CleanRibTmrP 0x41ee7104
PeerUpdTmrP 0x41ee70cc : DfrdNHTmrP 0x41ee7174 : DfrdRtselTmrP 0x41ee713c :
FastExtFallover 1 : FastIntFallover 0 : Enforce1stAS 1
PeerIdBitsP 0x41967120 : softOutSz 16 : RibUpdCtxCBP 0
UpdPeerCtxCBP 0 : UpdPeerCtxAFI 0 : TcpioCtxCB 0 : RedistBlk 1
NextCBPurg 1101119536 : NumPeerToPurge 0 : PeerIBGPCnt 0 : NonDet 0 :
DfrdPathSel 0
BGPRst 0 : NumGrCfg 1 : DfrdTmestmp 0 : SnmpTrps 0 : IgnrBestPthASP 0
RstOn 1 : RstMod 1 : RstRole 2 : AFFalgs 7 : RstInt 120 : MaxeorExtInt 361
FixedPartCrt 1 : VarParCrt 1
Packet Capture max allowed length 40960000 : current length 0

Peer Grp List
Nbr List
Confed Peer List
Address Family specific Information
AFIndex 0
NdSpFlag 0x41a190b0 : AFRttP 0x41a0d200 : NdRTMMkrP 0x41a19d28 : NdRTMAFTblVer
0 :
NdRibCtxAddr 1101110688
NdRibCtxAddrLen 255 : NdAFPrefix 0 : NdAfNLRIP 0 : NdAFNLRILen 0 : NdAFWPtrP 0
NdAFWLen 0 : NdAfNH : NdAFRedRttP 0x41a0d400 : NdRecCtxAdd 1101110868
NdRedCtxAddrLen 255 : NdAfRedMkrP 0x41a19e88 : AFAggRttP 0x41a0d600 :
AfAggCtxAddr
1101111028 : AfAggrCtxAddrLen 255
AfNumAggrPfx 0 : AfNumAggrASSet 0 : AfNumSuppmap 0 : AfNumAggrValidPfx 0 :
AfMPathRttP 0x41a0d700
MpathCtxAddr 1101111140 : MpathCtxAddrlen 255 : AfEorSet 0x41a19f98 :
NumDfrdPfx 0
AfActPeerHd 0x41a1a3a4 : AfExtDist 1101112312 : AfIntDist 200 : AfLocDist 200
AfNumRRc 0 : AfRR 0 : AfNetRttP 0x41a0d300 : AfNetCtxAddr 1101112392 :
AfNetCtxAddrlen 255
AfNwCtxAddr 1101112443 : AfNwCtxAddrlen 255 : AfNetBKDrRttP 0x41a0d500 :
AfNetBKDRCnt 0 : AfDampHLife 0
AfDampReuse 0 : AfDampSupp 0 : AfDampMaxHld 0 : AfDampCeiling 0 : AfDampRmapP
```

show ip bgp extcommunity-list

View information on all routes with Extended Community attributes.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast]
extcommunity-list [list name]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view information on all routes with extended community attributes corresponding to that VRF.
ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.

ipv4 *unicast*	(OPTIONAL) Enter the keywords `ipv4 unicast` to view information only related to ipv4 unicast routes.
ipv6 *unicast*	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
list name	Enter the extended community list name you wish to view. The range is 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

Example

```
Dell#show run extcommunity-list
!
ip extcommunity-list ecl1
 permit rt 100:4
 permit soo 40:4
Dell#show ip bgp extcommunity-list ecl1
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>  55.0.0.0/24        172.16.0.2                                0 200 i
*>  77.0.0.0/24        172.16.0.2                                0 200 i
Dell#show ip bgp extcommunity-list ec
```

```
% Error: Extended community list does not exist.

Dell#
```

show ip bgp filter-list

View the routes that match the filter lists.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] filter-list as-path-name
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view route information that matches the filter lists corresponding to that VRF.
ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
ipv4 *unicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
ipv6 *unicast*	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
as-path-name	Enter an AS-PATH access list name. The range is 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp filter-list hello` command shown in the following example.

Field	Description
Path source codes	Lists the path sources shown to the right of the last AS number in the Path column: • i = internal route entry • a = aggregate route entry • c = external confederation route entry • n = network route entry • r = redistributed route entry
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell#show run as-path a1
!
ip as-path access-list a1
 permit 500
Dell#

Dell#show ip bgp filter-list a1
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>  55.0.0.0/24        172.16.0.2                               0 200 400
500 600 i
*>  66.0.0.0/24        172.16.0.2                               0 200 500 i
```

show ip bgp flap-statistics

View flap statistics on BGP routes.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] flap-
statistics [ip-address [mask]] [filter-list as-path-name] [regexp regular-
expression]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view flap statistics on BGP routes corresponding to that VRF.

ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
ipv4 *unicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
ipv6 *unicast*	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
ip-address	(OPTIONAL) Enter the IP address (in dotted decimal format) of the BGP network to view information only on that network.
mask	(OPTIONAL) Enter the network mask (in slash prefix (`/x`) format) of the BGP network address.
filter-list *as-path-name*	(OPTIONAL) Enter the keyword `filter-list` then the name of a configured AS-PATH ACL. The range is 140 characters.
regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match. The range is 256 characters. • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (zero or more sequences). • `+` = (plus) the sequences in a pattern (one or more sequences). • `?` = (question mark) sequences in a pattern (either zero or one sequences). **NOTE: Enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.** • `[ ]` = (brackets) a range of single-character patterns. • `( )` = (parenthesis) groups a series of pattern elements to a single element. • `{ }` = (braces) minimum and the maximum match count. • `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp flap` command shown in the following example.

Field	Description
Network	Displays the network ID to which the route is flapping.
From	Displays the IP address of the neighbor advertising the flapping route.
Flaps	Displays the number of times the route flapped.
Duration	Displays the hours:minutes:seconds since the route first flapped.
Reuse	Displays the hours:minutes:seconds until the flapped route is available.
Path	Lists all the ASs the flapping route passed through to reach the destination network.

Example

```
Dell#show ip bgp flap-statistics
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            From                 Flaps       Duration
Reuse    Path
h   77.0.0.0/24        172.16.0.2               1   00:00:03         00:00:00
d   55.0.0.0/24        172.16.0.2               3   00:00:25         00:30:44
200 i
*>  66.0.0.0/24        172.16.0.2               1   00:00:23         00:00:00
200 i
Dell#*>n 66.66.77.77/32   0.0.0.0        0          32768 i
```

show ip bgp inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

C9000 Series

Syntax

```
show ip bgp [ipv4 unicast] inconsistent-as
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp inconsistent-as` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then local routes exist in the routing table.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight.
Path	Lists all the ASs the route passed through to reach the destination network.

Example

```
Dell>show ip bgp inconsistent-as
BGP table version is 280852, local router ID is 10.1.2.100
Status codes: s suppressed, d damped, h history, * valid, > best
Path source: I - internal, c - confed-external, r - redistributed, n - network
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network Next  Hop         Metric LocPrf Weight Path
*  3.0.0.0/8     63.114.8.33               0 18508 209 7018 80 i
*                63.114.8.34               0 18508 209 7018 80 i
*                63.114.8.60               0 18508 209 7018 80 i
*>               63.114.8.33               0 18508 701 80 i
*> 3.18.135.0/24 63.114.8.60               0 18508 209 7018 ?
*                63.114.8.34               0 18508 209 7018 ?
*                63.114.8.33               0 18508 701 7018 ?
*                63.114.8.33               0 18508 209 7018 ?
*> 4.0.0.0/8     63.114.8.60               0 18508 209 1 i
*                63.114.8.34               0 18508 209 1 i
*                63.114.8.33               0 18508 701 1 i
*                63.114.8.33               0 18508 209 1 i
*  6.0.0.0/20    63.114.8.60               0 18508 209 3549 i
*                63.114.8.34               0 18508 209 3549 i
*>               63.114.8.33      0        0 18508 ?
*                63.114.8.33               0 18508 209 3549 i
*  9.2.0.0/16    63.114.8.60               0 18508 209 701 i
*                63.114.8.34               0 18508 209 701 i
--More--
```

show ip bgp neighbors

Allows you to view the information BGP neighbors exchange.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast]
neighbors [ip-address [advertised-routes | dampened-routes | detail | flap-
statistics | routes | {received-routes [network [network-mask]]} | {denied-
routes [network [network-mask]]}]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view information exchanged by BGP neighbors corresponding to that VRF. **NOTE: You can use this attribute to view information exchanged by BGP neighbors that correspond to either a default or a non-default VRF.**
ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
ipv4 *unicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
ip-address	(OPTIONAL) Enter the IP address of the neighbor to view only BGP information exchanged with that neighbor.
advertised-routes	(OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keywords `dampened-routes` to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Enter the keyword `detail` to view neighbor-specific internal information for the IPv4 Unicast address family.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to view flap statistics on the neighbor's routes.
routes	(OPTIONAL) Enter the keyword `routes` to view only the neighbor's feasible routes.
received-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `received-routes` then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information received from neighbors. **NOTE: Configure the `neighbor soft-reconfiguration inbound` command prior to viewing all the information received from the neighbors.**
denied-routes [*network* [*network-mask*]	(OPTIONAL) Enter the keywords `denied-routes` then either the network address (in dotted decimal format) or the network mask (in slash prefix format) to view all information on routes denied via neighbor inbound filters.

Command Modes

- EXEC

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Added the `add-path` option to the S4810. Output on the S4810 shows the ADDPATH parameters.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Added the `detail` option. Output now displays the default MED value.
7.2.1.0	Added the `received` and `denied route` options.
6.3.10	The output is changed to display the total number of advertised prefixes.

Usage Information

After a peer reset, the contents of the notification log messages is displayed in hex values for debugging.

The neighbor information that this command displays does not include counts corresponding to ignored prefixes and updates. However, the martian case is an exception where neighbor information corresponding to ignored updates is displayed.

BGP shows the exact information that is exchanged between the BGP peers. It also indicates whether or not this information is received by the BGP peer.

The following describes the `show ip bgp neighbors` command shown in the following examples.

The Lines Beginning with:	Description
BGP neighbor	Displays the BGP neighbor address and its AS number. The last phrase in the line indicates whether the link between the BGP router and its neighbor is an external or internal one. If they are located in the same AS, the link is internal; otherwise the link is external.
BGP version	Displays the BGP version (always version 4) and the remote router ID.
BGP state	Displays the neighbor's BGP state and the amount of time in hours:minutes:seconds it has been in that state.
Last read	This line displays the following information:

The Lines Beginning with:	Description
	• last read is the time (hours:minutes:seconds) the router read a message from its neighbor • hold time is the number of seconds configured between messages from its neighbor • keepalive interval is the number of seconds between keepalive messages to help ensure that the TCP session is still alive.
Received messages	This line displays the number of BGP messages received, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Sent messages	The line displays the number of BGP messages sent, the number of notifications (error messages), and the number of messages waiting in a queue for processing.
Received updates	This line displays the number of BGP updates received and sent.
Soft reconfiguration	This line indicates that soft reconfiguration inbound is configured.
Minimum time	Displays the minimum time, in seconds, between advertisements.
(list of inbound and outbound policies)	Displays the policy commands configured and the names of the Route map, AS-PATH ACL, or Prefix list configured for the policy.
For address family:	Displays the IPv4 Unicast as the address family.
BGP table version	Displays which version of the primary BGP routing table the router and the neighbor are using.
accepted prefixes	Displays the number of network prefixes the router accepts and the amount of memory used to process those prefixes.
Prefix advertised	Displays the number of network prefixes advertised, the number rejected, and the number withdrawn from the BGP routing table.
Connections established	Displays the number of TCP connections established and dropped between the two peers to exchange BGP information.
Last reset	Displays the amount of time since the peering session was last reset. Also states if the peer resets the peering session. If the peering session was never reset, the word never is displayed.
Local host:	Displays the peering address of the local router and the TCP port number.
Foreign host:	Displays the peering address of the neighbor and the TCP port number.

Example

```
Dell#show ip bgp neighbors 172.16.0.2
BGP neighbor is 172.16.0.2, remote AS 200, external link
  Member of peer-group port0 for session parameters
  BGP remote router ID 172.16.0.2
  BGP state ESTABLISHED, in this state for 00:13:55
  Last read 00:00:03, Last write 00:00:55
  Hold time is 180, keepalive interval is 60 seconds
  Received 50 messages, 0 in queue
     1 opens, 0 notifications, 34 updates
     15 keepalives, 0 route refresh requests
  Sent 18 messages, 0 in queue
     1 opens, 0 notifications, 0 updates
     16 keepalives, 0 route refresh requests

  Route refresh request: received 0, sent messages 1
  Minimum time between advertisement runs is 30 seconds
  Minimum time before advertisements start is 0 seconds

  Capabilities received from neighbor for IPv4 Unicast :
```

```
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)



  Capabilities advertised to neighbor for IPv4 Unicast :
    MULTIPROTO_EXT(1)
    ROUTE_REFRESH(2)
    ADD_PATH(69)
    CISCO_ROUTE_REFRESH(128)



  For address family: IPv4 Unicast
  BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
  InQ : Added 0, Replaced 0, Withdrawn 0
  OutQ : Added 0, Withdrawn 0
  Allow local AS number 0 times in AS-PATH attribute
  Prefixes accepted 2, withdrawn 15 by peer, martian prefixes ignored 0
  Prefixes advertised 0, denied 0, withdrawn 0 from peer

  Connections established 1; dropped 0
  Last reset never
Local host: 172.16.0.1, Local port: 58145
Foreign host: 172.16.0.2, Foreign port: 179

Dell#
```

Related Commands show ip bgp — views the current BGP routing table.

show ip bgp next-hop

View all next hops (using learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

C9000 Series

Syntax `show ip bgp [vrf vrf-name] next-hop`

Parameters

vrf *vrf-name*	Enter the keyword `vrf` followed by the name of the VRF to view all next hops corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information The following describes the `show ip bgp next-hop` command shown in the following example.

Field	Description
Next-hop	Displays the next-hop IP address.
Via	Displays the IP address and interface used to reach the next hop.
RefCount	Displays the number of BGP routes using this next hop.
Cost	Displays the cost associated with using this next hop.
Flaps	Displays the number of times the next hop has flapped.
Time Elapsed	Displays the time elapsed since the next hop was learned. If the route is down, this field displays time elapsed since the route went down.

Example

```
Dell#   show ip bgp next-hop
     Next-hop            Resolved
    172.16.0.2             YES
Dell#
```

show ip bgp paths

View all the BGP path attributes in the BGP database.

C9000 Series

Syntax `show ip bgp paths [regexp regular-expression]`

Parameters

regexp *regular-expression* Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (zero or more sequences).
- `+` = (plus) the sequences in a pattern (one or more sequences).
- `?` = (question mark) sequences in a pattern (either zero or one sequences).

> **NOTE: Enter an escape sequence (CTRL+v) prior to entering the ? regular expression.**

- `[ ]` = (brackets) a range of single-character patterns.
- `( )` = (parenthesis) groups a series of pattern elements to a single element.
- `{ }` = (braces) minimum and the maximum match count.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp path` command shown in the following example.

Field	Description
Total	Displays the total number of BGP path attributes.
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using this path attribute.
Metric	Displays the MED attribute for this path attribute.
Path	Displays the AS path for the route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

Example

```
Dell#show ip bgp path
Total 16 Paths
Address      Hash Refcount   Metric Path
0x1efe7e5c   15       10000          32 ?
0x1efe7e1c   71       10000          23 ?
0x1efe7ddc   127      10000          22 ?
0x1efe7d9c   183      10000          43 ?
0x1efe7d5c   239      10000          42 ?
0x1efe7c9c   283          6          {102 103} ?
0x1efe7b1c   287        336 20000    ?
0x1efe7d1c   295      10000          13 ?
0x1efe7c5c   339          6          {92 93} ?
```

```
0x1efe7cdc   351      10000          12 ?
0x1efe7c1c   395          6          {82 83} ?
0x1efe7bdc   451          6          {72 73} ?
0x1efe7b5c   491         78       0  ?
0x1efe7adc   883          2     120  i
0x1efe7e9c   983      10000          33 ?
0x1efe7b9c   1003         6       0  i
Dell#
```

show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

C9000 Series

Syntax

```
show ip bgp paths as-path
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp paths as-path` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these AS-Paths.
AS-Path	Displays the AS paths for this route, with the origin code for the route listed last. Numbers listed between braces {} are AS_SET information.

Example

```
Dell# show ip bgp paths as-path
Total 13 AS-Paths
Address      Hash Refcount AS-Path
0x1ea3c1ec   251         1   42
```

```
0x1ea3c25c   251         1   22
0x1ea3c1b4   507         1   13
0x1ea3c304   507         1   33
0x1ea3c10c   763         1   {92 93}
0x1ea3c144   763         1   {102 103}
0x1ea3c17c   763         1   12
0x1ea3c2cc   763         1   32
0x1ea3c09c   764         1   {72 73}
0x1ea3c0d4   764         1   {82 83}
0x1ea3c224   1019        1   43
0x1ea3c294   1019        1   23
0x1ea3c02c   1021        4
Dell#
```

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

C9000 Series

Syntax `show ip bgp [vrf vrf-name] paths community`

Parameters

vrf *vrf-name* (OPTIONAL) Enter the keyword `vrf` to view all unique COMMUNITY numbers in the BGP database corresponding to that VRF.

NOTE: You can use this attribute to view information on unique COMMUNITY numbers in a BGP database that correspond to either a default or a non-default VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Version	Description
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp paths community` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these communities.
Community	Displays the community attributes in this BGP path.

Example

```
Dell#show ip bgp paths community
Total 2 communities
Refcount   Community
1          NO-ADVERTISE
1          200:1        1000:1       3000:1
```

show ip bgp peer-group

View information on the BGP peers in a peer group.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] peer-group [peer-group-name [detail | summary]]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` to view information on BGP peers in a peer group corresponding to that VRF. **NOTE: You can use this attribute to view information on BGP peers in a peer group that correspond to either a default or a non-default VRF.**
ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
ipv4 *unicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.
peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword `detail` to view detailed status information of the peers in that peer group.
summary	(OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in the `show ip bgp summary` command.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters. Introduced on S6000–ON.
9.4.(0.0)	Added support for VRF.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Added the `add-path` option to the S4810. Output on the S4810 shows the ADDPATH parameters.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp peer-group` command shown in the following example.

Line beginning with:	Description
Peer-group	Displays the peer group's name.
Administratively shut	Displays the peer group's status if the peer group is not enabled. If you enable the peer group, this line is not displayed.
BGP version	Displays the BGP version supported.
Minimum time	Displays the time interval between BGP advertisements.
For address family	Displays IPv4 Unicast as the address family.
BGP neighbor	Displays the name of the BGP neighbor.
Number of peers	Displays the number of peers currently configured for this peer group.
Peer-group members:	Lists the IP addresses of the peers in the peer group. If the address is outbound optimized, an * is displayed next to the IP address.

Example

```
Dell#show ip bgp peer-group
Peer-group port0, remote AS 200
BGP version 4
Minimum time between advertisement runs is 30 seconds
For address family: IPv4 Unicast
BGP neighbor is port0, peer-group external
Update packing has 4_OCTET_AS support enabled

Number of peers in this group 1
```

```
Maximum limit on the accepted connections 256


 Peer-group members (* - outbound optimized):
172.16.0.2
Dell#
```

Related Commands

- neighbor peer-group (assigning peers) — assigns a peer to a peer-group.
- neighbor peer-group (creating group) — creates a peer group

show ip bgp regexp

Display the subset of the BGP routing tables matching the regular expressions specified.

C9000 Series

Syntax `show ip bgp [vrf vrf-name] regexp regular-expression [character]`

Parameters

vrf *vrf-name*

Enter the keyword `vrf` and then the name of the VRF to view the subset of BGP routing tables that match the regular expression specified on that VRF.

NOTE: You can use this attribute to view the subset of BGP routing tables that match the regular expression that is specified on either a default or a non-default VRF.

***regular-expression* [*character*]**

Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (zero or more sequences).
- `+` = (plus) the sequences in a pattern (one or more sequences).
- `?` = (question mark) sequences in a pattern (either zero or one sequences).

  NOTE: Enter an escape sequence (CTRL+v) prior to entering the `?` regular expression.
- `[ ]` = (brackets) a range of single-character patterns.
- `( )` = (parenthesis) groups a series of pattern elements to a single element.
- `{ }` = (braces) minimum and the maximum match count.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Introduced on the S6000–ON.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

The following describes the `show ip bgp regexp` command shown in the following example.

Field	Description
Network	Displays the destination network prefix of each BGP route.
Next Hop	Displays the next hop address of the BGP router. If 0.0.0.0 is listed in this column, then non-BGP routes exist in the router's routing table.
Metric	Displays the BGP router's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.
Weight	Displays the route's weight
Path	Lists all the AS paths the route passed through to reach the destination network.

Example

```
Dell#show ip bgp regexp ^200
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            Next Hop            Metric     LocPrf Weight Path
*>  55.0.0.0/24        172.16.0.2                               0 200 i
*>  66.0.0.0/24        172.16.0.2                               0 200 i
```

show ip bgp summary

View the status of all BGP connections.

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] summary
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view the status of all BGP connections corresponding to that VRF.
ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` and specify `multicast` option to view information related only to ipv4 multicast routes.
ipv4 *unicast*	(OPTIONAL) Enter the keyword `ipv4` and specify `unicast` option to view information related only to ipv4 unicast routes.
ipv6 *unicast*	(OPTIONAL) Enter the keyword `ipv6` and specify `unicast` option to view information related only to ipv6 unicast routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

In BGP, route attributes are maintained at different locations. When attributes that correspond to multiple routes change, then attribute counts that the `show ip bgp summary` command displays are calculated as summations of attributes corresponding to all the associated routes. For example, if cluster_id is an attribute associated with 1000 routes that contain the same set of attributes, then the cluster_id count is 1. If these 1000 routes are set with different attribute values with the same cluster_id, then the cluster_id count is 1000, since the same value is stored for1000 different attribute records.

The attribute next-hop is a part of the BGP attribute data structure.

If two peers send the same route that contains similar path attributes, then two entries are maintained in the back-end, as both these entries have different next-hops. If this same route is sent to a different peer, an entry for each peer is created, as the next-hop is different. As a result, the BGP attributes count in the summary output differs accordingly.

The following describes the `show ip bgp summary` command shown in the following example.

Field	Description
BGP router identifier	Displays the local router ID and the AS number.
BGP table version	Displays the BGP table version and the main routing table version.
network entries	Displays the number of network entries, route paths, and the amount of memory used to process those entries.
paths	Displays the number of paths and the amount of memory used.
denied paths	Displays the number of denied paths and the amount of memory used.
BGP path attribute entries	Displays the number of BGP path attributes and the amount of memory used to process them.
BGP AS-PATH entries	Displays the number of BGP AS_PATH attributes processed and the amount of memory used to process them.
BGP community entries	Displays the number of BGP COMMUNITY attributes processed and the amount of memory used to process them. The `show ip bgp community` command provides more details on the COMMUNITY attributes.
Dampening enabled	Displayed only when you enable dampening. Displays the number of paths designated as history, dampened, or penalized.
Neighbor	Displays the BGP neighbor address.
AS	Displays the AS number of the neighbor.
MsgRcvd	Displays the number of BGP messages that neighbor received.
MsgSent	Displays the number of BGP messages that neighbor sent.
TblVer	Displays the version of the BGP table that was sent to that neighbor.
InQ	Displays the number of messages from that neighbor waiting to be processed.
OutQ	Displays the number of messages waiting to be sent to that neighbor. If a number appears in parentheses, the number represents the number of messages waiting to be sent to the peer group.
Up/Down	Displays the amount of time that the neighbor is in the Established stage. If the neighbor has never moved into the Established stage, the word, "never", is displayed. The output format is:

Time Established	Display Example
< 1 day	00:12:23 (hours:minutes:seconds)
< 1 week	1d21h (DaysHours)
> 1 week	11w2d (WeeksDays)

State/Pfxrcd	If the neighbor is in Established stage, the number of network prefixes received. If a maximum limit was configured with the `neighbor maximum-prefix` command, (prfxd) appears in this column.

Field	Description
	If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm). When the peer is transitioning between states and clearing the routes received, the phrase (Purging) may appear in this column. If the neighbor is disabled, the phrase (Admin shut) appears in this column.

Example

```
Dell#show ip bgp summary
BGP router identifier 192.168.11.5, local AS number 100
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
2 network entrie(s) using 152 bytes of memory
2 paths using 208 bytes of memory
BGP-RIB over all using 210 bytes of memory
2 BGP path attribute entrie(s) using 144 bytes of memory
1 BGP AS-PATH entrie(s) using 10 bytes of memory
2 neighbor(s) using 16384 bytes of memory

Neighbor        AS            MsgRcvd  MsgSent     TblVer  InQ  OutQ Up/Down
State/Pfx
172.16.0.2      200                10        8          0    0     0 00:05:34
2
192.168.10.2    100                 0       22          0    0     0 00:00:00
(shut)
Dell#
```

show running-config bgp

To display the current BGP configuration, use this feature.

C9000 Series

Syntax `show running-config bgp`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Version	Description
7.6.1.0	Introduced on the E-Series.

timers bgp

Adjust the BGP Keep Alive and Hold Time timers.

C9000 Series

Syntax

`timers bgp` *`keepalive holdtime`*

To return to the default, use the `no timers bgp` command.

Parameters

keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is from 1 to 65535. The default is **60 seconds**.
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is from 3 to 65535. The default is **180 seconds**.

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

timers bgp extended

Adjust the BGP idle holdtime for all the BGP neighbors.

Syntax

`timers bgp extended idle-holdtime`

To return to the default, use the `no timers bgp extended` command.

Parameters

extended *idle-holdtime*	Enter a number for the time interval, in seconds, for the peer to be idle state. The range is from 1 to 32767. The default is **15 seconds**.

Defaults

The default *idle-holdtime* is **15 seconds**.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the C9010, MXL, FN IOM, S3100 series, S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000, S6010–ON, S6100–ON, Z9100–ON, Z9500, and S6000–ON.

Usage Information

The peer remains in idle state based on the configured `idle-holdtime`. The less the `idle-holdtime`, lesser the peer in idle state.

For the new *idle-holdtime* to take effect, you need to shutdown all the peers manually using `neighbor shutdown` command and enable the peers again.

MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables multicast routing policy throughout the internet and connecting multicast topologies between BGP and autonomous systems (ASs).

MBGP on the Dell Networking OS is implemented as per IETF RFC 1858.

BGPv4 is supported in the following:

Version	Platform Support
9.9(0.0)	C9010
9.2(1.0)	Z9500
7.8.1.0	TeraScale and C-Series (MBGP for IPv6)
7.8.1.0	S-Series (MBGP for IPv4 Multicast Only)
8.2.1.0	E-Series ExaScale (MBGP)

debug ip bgp dampening

View information on routes being dampened.

C9000 Series

Syntax

`debug ip bgp [vrf vrf-name] [ipv4 {unicast | multicast} | ipv6 unicast] dampening`

To disable debugging, use the `no debug ip bgp dampening` command.

Parameters

vrf *vrf-name*	Enter the keyword `vrf` followed by the name of the VRF to view information on dampened routes corresponding to that VRF.
ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view dampened-route information related only to ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view dampened-route information related only to ipv4 unicast routes.
ipv6 *unicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `unicast` to view dampened-route information related only to ipv6 unicast routes.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

b

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced IPv6 MGBP support for the E-Series.

distance bgp

Configure three administrative distances for routes.

C9000 Series

Syntax

`distance bgp external-distance internal-distance local-distance`

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is from 1 to 255. The default is **20**.
internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is from 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the network command. The range is from 1 to 255. The default is **200**.

Defaults

- external-distance = **20**
- internal-distance = **200**
- local-distance = **200**

Command Modes

ROUTER BGP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

CAUTION: Dell Networking recommends not changing the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table. Routes from confederations are treated as internal BGP routes.

Related Commands

router bgp — enters ROUTER mode on the switch.

show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

C9000 Series

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast]
dampened-paths
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keywords `vrf` and then the name of the VRF to view routes that are affected by a specific community list corresponding to that VRF.
ipv4 *multicast*	(OPTIONAL) Enter the keyword `ipv4` followed by the keyword `multicast` to view information related only to ipv4 multicast routes.
ipv4 *unicast*	(OPTIONAL) Enter the keywords `ipv4` followed by the keyword `unicast` to view information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword `ipv6` followed by the keyword `unicast` to view information related only to ipv6 unicast routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048–ON and S4048–ON.
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
9.4(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

To determine a BGP session flap, both a route-down event and a subsequent route-up event corresponding to a single route are considered. As a result, a flap event is penalized only one time during the route-down event. The subsequent route-up event corresponding to the same route is not considered as a flap and is not penalized.

The history paths that the `show ip bgp` command displays contain only the prefix and the next-hop information. The next-hop information shows the ip address of the neighbor. It does not show the actual next-hop details.

The following describes the `show ip bgp damp` command shown in the following example.

Field	Description
Network	Displays the network ID to which the route is dampened.
From	Displays the IP address of the neighbor advertising the dampened route.
Reuse	Displays the hour:minutes:seconds until the dampened route is available.
Path	Lists all the ASs the dampened route passed through to reach the destination network.

Example

```
Dell#show ip bgp dampened-paths
BGP local RIB : Routes to be Added 0, Replaced 0, Withdrawn 0
BGP local router ID is 192.168.11.5
Status codes: s suppressed, S stale, d dampened, h history, * valid, > best
Path source: I - internal, a - aggregate, c - confed-external, r -
redistributed
             n - network,  D - denied,  S - stale
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network            From            Reuse     Path

d   55.0.0.0/24      172.16.0.2             00:36:23      200

Dell#
```

BGP Extended Communities (RFC 4360)

BGP Extended Communities, as defined in RFC 4360, is an optional transitive BGP attribute.

BGP Extended Communities provides two major advantages over Standard Communities:

- The range is extended from 4-octet (AA:NN) to 8-octet (Type:Value) to provide enough number communities.
- Communities are structured using a new "Type" field (1 or 2-octets), allowing you to provide granular control/filter routing information based on the type of extended communities.

deny

To reject (deny) from the two types of extended communities, route origin (rt) or site-of-origin (soo), use this feature.

C9000 Series

Syntax

`deny {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN}`

To remove (delete) the rule, use the `no deny {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN}` command.

Parameters

rt	Enter the keyword `rt` to designate a Route Origin community.
soo	Enter the keyword `soo` to designate a Site-of-Origin community (also known as Route Origin).

as4 *ASN4:NN*	Enter the keyword `as4` then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Related Commands permit — configures to add (permit) rules.

show ip extcommunity-list — displays the extended community list.

deny regex

This feature allows you to specify an extended community to reject (deny) using a regular expression (regex).

C9000 Series

Syntax `deny regex {regex}`

To remove, use the `no deny regex {regex}` command.

Parameters

regex	Enter a regular expression.

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information Duplicate commands are silently accepted.

Example

```
Dell(conf-ext-community-list)#deny regexp 123
Dell(conf-ext-community-list)#
```

Related Commands permit regex — permits a community using a regular expression.

description

To designate a meaningful description to the extended community, use this feature.

C9000 Series

Syntax `description {line}`

To remove the description, use the `no description {line}` command.

Parameters

line	Enter a description (maximum 80 characters).

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

ip extcommunity-list

To enter the Extended Community-list mode, use this feature.

C9000 Series

Syntax

`ip extcommunity-list word`

To exit from this mode, use the `exit` command.

Parameters

word	Enter a community list name (maximum 16 characters).

Defaults

none

Command Modes

CONFIGURATION (conf-ext-community-list)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

This mode changes the prompt.

Example

```
Dell(conf)#ip extcommunity-list test
Dell(conf-ext-community-list)#
```

match extcommunity

To match an extended community in the Route Map mode, use this feature.

C9000 Series

Syntax

`match extcommunity {extended community list name}`

To change the match, use the `no match extcommunity {extended community list name}` command.

Parameters

extended community list name	Enter the name of the extended community list.

Defaults none

Command Modes ROUTE MAP (config-route-map)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information Like standard communities, you can use extended communities in the route-map to match the attribute.

Example

```
Dell(config-route-map)#match extcommunity Freedombird
Dell(config-route-map)#
```

permit

To add rules (permit) from the two types of extended communities, Route Origin (rt) or Site-of-Origin (soo), use this feature.

C9000 Series

Syntax `permit {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN}`

To change the rules, use the `no permit {rt | soo} {as4 ASN4:NN | ASN:NNNN | IPADDR:NN}` command.

Parameters

rt	Enter the keyword `rt` to designate a Route Origin community.
soo	Enter the keyword `soo` to designate a Site-of-Origin community (also known as Route Origin).
as4 *ASN4:NN*	Enter the keyword `as4` then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Related Commands deny — configures to delete (deny) rules.

show ip bgp extcommunity-list — displays the extended community list.

permit regex

This feature allows you specify an extended community to forward (permit) using a regular expression (regex).

C9000 Series

Syntax `permit regex {regex}`

To remove, use the `no permit regex {regex}` command.

Parameters

regex	Enter a regular expression.

Defaults Not configured.

Command Modes CONFIGURATION (conf-ext-community-list)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Version	Description
7.6.1.0	Introduced on the E-Series.

Usage Information Duplicate commands are silently accepted.

Example

```
Dell(conf-ext-community-list)#permit regexp 123
Dell(conf-ext-community-list)#
```

Related Commands deny regex — denies a community using a regular expression.

set extcommunity rt

To set Route Origin community attributes in Route Map, use this feature.

C9000 Series

Syntax `set extcommunity rt {as4 ASN4:NN [non-trans] | ASN:NNNN [non-trans] | IPADDR:NN [non-trans]} [additive]`

To delete the Route Origin community, use the `no set extcommunity` command.

Parameters

as4 *ASN4:NN*	Enter the keyword `as4` then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).
additive	(OPTIONAL) Enter the keyword `additive` to add to the existing extended community.
non-trans	(OPTIONAL) Enter the keywords `non-trans` to indicate a non-transitive BGP extended community.

Defaults none

Command Modes ROUTE MAP (config-route-map)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T
8.3.11.1	Introduced on the Z-9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Version	Description
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

If the set community `rt` and `soo` are in the same route-map entry, the behavior defines as:

- If the `rt` option comes before `soo`, with or without the `additive` option, `soo` overrides the communities `rt` sets.
- If the `rt` option comes after `soo`, without the `additive` option, `rt` overrides the communities `soo` sets.
- If the `rt` with the `additive` option comes after `soo`, `rt` adds the communities `soo` sets.

Related Commands

set extcommunity soo — sets the extended community site-of-origin in the route-map.

set extcommunity soo

To set extended community site-of-origin in Route Map, use this feature.

C9000 Series

Syntax

`set extcommunity soo {as4 ASN4:NN | ASN:NNNN | IPADDR:NN [non-trans]}`

To delete the site-of-origin community, use the `no set extcommunity` command.

Parameters

as4 *ASN4:NN*	Enter the keyword `as4` then the 4-octet AS specific extended community number in the format ASN4:NN (4-byte AS number:2-byte community value).
ASN:NNNN	Enter the 2-octet AS specific extended community number in the format ASN:NNNN (2-byte AS number:4-byte community value).
IPADDR:NN	Enter the IP address specific extended community in the format IPADDR:NN (4-byte IPv4 Unicast Address:2-byte community value).
non-trans	(OPTIONAL) Enter the keywords `non-trans` to indicate a non-transitive BGP extended community.

Defaults

none

Command Modes

ROUTE MAP (config-route-map)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

If the set community `rt` and `soo` are in the same route-map entry, the behavior defines as:

- If the `rt` option comes before `soo`, with or without the `additive` option, `soo` overrides the communities `rt` sets.
- If the `rt` option comes after `soo`, without the `additive` option, `rt` overrides the communities `soo` sets.
- If the `rt` with the `additive` option comes after `soo`, `rt` adds the communities `soo` sets.

Related Commands

set extcommunity rt — sets the extended community route origins using the route-map.

show ip bgp ipv4 extcommunity-list

To display the IPv4 routes matching the extended community list name, use this feature.

C9000

Syntax

```
show ip bgp [ipv4 [multicast | unicast] | ipv6 unicast] extcommunity-list name
```

Parameters

multicast	Enter the keyword `multicast` to display the multicast route information.
unicast	Enter the keyword `unicast` to display the unicast route information.
ipv6 unicast	Enter the keywords `ipv6 unicast` to display the IPv6 unicast route information.
name	(OPTIONAL) Enter the name of the extcommunity-list.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Version	Description
7.6.1.0	Introduced on the E-Series.

Usage Information

If there is a type or sub-type that is not well-known, it is displayed as:`TTSS:XX:YYYY`.

Where TT is type, SS is sub-type displayed in hexadecimal format, XX:YYYY is the value divided into 2–byte and 4-byte values in decimal format. This format is consistent with other vendors.

For example, if the extended community has type 0x04, sub-type 0x05, value 0x20 00 00 00 10 00, it displays as: `0x0405:8192:4096`.

Non-transitive extended communities are marked with an asterisk.

Example

```
Dell#show ip bgp ipv4 multicast extcommunity-list
BGP routing table entry for 192.168.1.0/24, version 2

Paths: (1 available, table Default-IP-Routing-Table.)
Not advertised to any peer
Received from :
  100.100.1.2 (2.4.0.1) Best
    AS_PATH : 200
    Next-Hop : 100.100.1.2, Cost : 0
    Origin IGP, Metric 4294967295 (Default), LocalPref 100, Weight 0,
external
    Communities :
    300:400 500:600

    Extended Communities :
    RT:1111:4278080 SoO:35:4 SoO:36:50529043 SoO:37:50529044
    SoO:38:50529045 SoO:0.0.0.2:33 SoO:506.62106:34 0x0303:254:11223*

Dell#
```

show ip bgp paths extcommunity

To display all BGP paths having extended community attributes, use this feature.

C9000 Series

Syntax

```
show ip bgp paths extcommunity
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip bgp paths extcommunity` command shown in the following example.

Field	Description
Address	Displays the internal address where the path attribute is stored.
Hash	Displays the hash bucket where the path attribute is stored.
Refcount	Displays the number of BGP routes using these extended communities.
Community	Displays the extended community attributes in this BGP path.

Example

```
Dell# show ip bgp paths extcommunity
Total 1 Extended Communities

Address     Hash  Refcount Extended Community
0x41d57024  12272 1        RT:7:200 SoO:5:300 SoO:0.0.0.3:1285

Dell#
```

show ip extcommunity-list

Display the IP extended community list.

C9000 Series

Syntax

```
show ip extcommunity-list [word]
```

Parameters

word	Enter the name of the extended community list you want to view.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Example

```
Dell# show ip extcommunity-list test
ip extcommunity-list test
  deny RT:1234:12
  permit regexp 123
  deny regexp 234
  deny regexp 123
Dell#
```

show running-config extcommunity-list

To display the current configuration of the extended community lists, use this feature.

C9000 Series

Syntax `show running-config extcommunity-list [word]`

Parameters

word	Enter the name of the extended community list you want to view.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Example

```
Dell# show running-config extcommunity-list test

ip extcommunity-list test
  permit rt 65033:200
  deny soo 101.11.11.2:23
  permit rt as4 110212:340
  deny regex ^(65001_)$
```

```
Dell#
```

IPv6 BGP Commands

IPv6 border gateway protocol (IPv6 BGP) is an external gateway protocol that transmits interdomain routing information with extended IP address space within and between Autonomous Systems (AS).

Basically, two routers (called neighbors or peers) exchange information including full routing tables and periodically send messages to update those routing tables.

address-family

Enable the IPv4 multicast or the IPv6 address family.

C9000 Series

Syntax `address-family [ipv4 multicast| ipv6unicast]`

Parameters

ipv4multicast	Enter BGPv4 multicast mode.
ipv6unicast	Enter BGPv6 mode.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
6.5.1.0	Introduced

Usage Information Enter `ipv6unicast` to enter the BGP for IPv6 mode (CONF-ROUTER_BGPv6_AF).

address family ipv6 unicast

This command changes the context to subsequent address family identifier (SAFI).

C9000 Series

Syntax `address family ipv6 unicast`

To remove SAFI context, use the `no address family ipv6 unicast` command.

Parameters

ipv6	Enter the keyword `ipv6` to specify the address family as IPv6.
unicast	Enter the keyword `unicast` to specify multicast as SAFI.

Defaults IPv6 Unicast

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced

Usage Information All subsequent commands apply to this address family after you execute this command. You can exit from this AFI/SAFI to the IPv6 Unicast (the default) family by entering `exit` and returning to the Router BGP context.

aggregate-address

Summarize a range of prefixes to minimize the number of entries in the routing table.

C9000 Series

Syntax `aggregate-address` *`ipv6-address prefix-length`* `[advertise-map` *`map-name`*`] [as-set] [attribute-map` *`map-name`*`] [summary-only] [suppress-map` *`map-name`*`]`

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
advertise-map *map-name*	(OPTIONAL) Enter the keywords `advertise-map` followed by the name of a configured route map to set filters for advertising an aggregate route.
as-set	(OPTIONAL) Enter the keywords `as-set` to generate path attribute information and include it in the aggregate. AS_SET includes AS_PATH and community information from the routes included in the aggregated route.
attribute-map *map-name*	(OPTIONAL) Enter the keywords `attribute-map` followed by the name of a configured route map to modify attributes of the aggregate, excluding AS_PATH and NEXT_HOP attributes.
summary-only	(OPTIONAL) Enter the keywords `summary-only` to advertise only the aggregate address. Specific routes will not be advertised.
suppress-map *map-name*	(OPTIONAL) Enter the keywords `suppress-map` followed by the name of a configured route map to identify which more-specific routes in the aggregate are suppressed.

Defaults Not configured.

Command Modes CONFIGURATION-ROUTER-BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

At least one of the routes included in the aggregate address must be in the BGP routing table for the configured aggregate to become active.

Do not add the `as-set` parameter to the aggregate if routes within the aggregate are constantly changing as the aggregate will flap to keep track of the changes in the AS_PATH.

In route maps used in the `suppress-map` parameter, routes meeting the `deny` clause are not suppress; in other words, they are allowed. The opposite is true: routes meeting the `permit` clause are suppressed.

If the route is injected via the network command, that route still appears in the routing table if the `summary-only` parameter is configured in the `aggregate-address` command.

The `summary-only` parameter suppresses all advertisements. If you want to suppress advertisements to only specific neighbors, use the `neighbor distribute-list` command.

In the `show ip bgp` command, aggregates contain an 'a' in the first column and routes suppressed by the aggregate contain an 's' in the first column.

bgp always-compare-med

Allows you to enable comparison of the MULTI_EXIT_DISC (MED) attributes in the paths from different external ASs.

C9000 Series

Syntax

`bgp always-compare-med`

To disable comparison of MED, use the `no bgp always-compare-med` command.

Defaults

Disabled (that is, the software only compares MEDs from neighbors within the same AS).

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

Any update without a MED attribute is the least preferred route.

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath as-path ignore

Ignore the AS PATH in BGP best path calculations.

C9000 Series

Syntax

```
bgp bestpath as-path ignore
```

To return to the default, use the `no bgp bestpath as-path ignore` command.

Defaults

Disabled (that is, the software considers the AS_PATH when choosing a route as best).

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath med confed

Enable MULTI_EXIT_DISC (MED) attribute comparison on paths learned from BGP confederations.

C9000 Series

Syntax

```
bgp bestpath med confed
```

To disable MED comparison on BGP confederation paths, use the `no bgp bestpath med confed` command.

Defaults

Disabled

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

The software compares the MEDs only if the path contains no external autonomous system numbers.

If you enable this command, use the `clear ip bgp *` command to recompute the best path.

bgp bestpath med missing-as-best

During path selection, indicate preference to paths with missing MED (MULTI_EXIT_DISC) over those paths with an advertised MED attribute.

C9000 Series

Syntax `bgp bestpath med missing-as-best`

To return to the default selection, use the `no bgp bestpath med missing-as-best` command.

Defaults Disabled

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information The MED is a 4-byte unsigned integer value and the default behavior is to assume a missing MED as 4294967295. This command causes a missing MED to be treated as 0. During the path selection, paths with a lower MED are preferred over those with a higher MED.

bgp client-to-client reflection

Allows you to enable route reflection between clients in a cluster.

C9000 Series

Syntax `bgp client-to-client reflection`

To disable client-to-client reflection, use the `no bgp client-to-client reflection` command.

Defaults Enabled when a route reflector is configured.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.4.1.0	Introduced

Usage Information Route reflection to clients is not necessary if all client routers are fully meshed.

Related Commands

- bgp cluster-id – assigns an ID to a BGP cluster with two or more route reflectors.
- neighbor route-reflector-client – configures a route reflector and clients.

bgp cluster-id

Assign a cluster ID to a BGP cluster with more than one route reflector.

C9000 Series

Syntax `bgp cluster-id {ip-address | number}`

To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

Parameters

ip-address	Enter an IP address as the route reflector cluster ID.
number	Enter a route reflector cluster ID as a number from 1 to 4294967295.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information When a BGP cluster contains only one route reflector, the cluster ID is the route reflector's router ID. For redundancy, a BGP cluster may contain two or more route reflectors and you assign a cluster ID with the `bgp cluster-id` command. Without a cluster ID, the route reflector cannot recognize route updates from the other route reflectors within the cluster.

The default format for displaying the cluster-id is dotted decimal, but if you enter the `cluster-id` as an integer, it is displayed as an integer.

Related Commands

- bgp client-to-client reflection – enables route reflection between route reflector and clients.
- neighbor route-reflector-client – configures a route reflector and clients.
- show ip bgp cluster-list – views paths with a cluster ID.

bgp confederation identifier

Configure an identifier for a BGP confederation.

C9000 Series

Syntax

`bgp confederation identifier as-number`

To delete a BGP confederation identifier, use the `no bgp confederation identifier as-number` command.

Parameters

as-number	Enter the AS number. The range is 1 to 65535.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

The autonomous systems configured in this command are visible to the EBGP neighbors. Each autonomous system is fully meshed and contains a few connections to other autonomous systems. The next hop, MED, and local preference information is preserved throughout the confederation.

The system accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

bgp dampening

Enable BGP route dampening and configure the dampening parameters.

C9000 Series

Syntax

`bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]`

To disable route dampening, use the `no bgp dampening [half-life reuse suppress max-suppress-time] [route-map map-name]` command.

Parameters

half-life	(OPTIONAL) Enter the number of minutes after which the Penalty is decreased. After the router assigns a Penalty of 1024 to a route, the Penalty is decreased by half after the half-life period expires. The range is 1 to 45. The default is **15 minutes**.

	reuse	(OPTIONAL) Enter a number as the reuse value, which is compared to the flapping route's Penalty value. If the Penalty value is less than the reuse value, the flapping route is once again advertised (or no longer suppressed). The range is 1 to 20000. The default is **750**.
	suppress	(OPTIONAL) Enter a number as the suppress value, which is compared to the flapping route's Penalty value. If the Penalty value is greater than the suppress value, the flapping route is no longer advertised (that is, it is suppressed). The range is 1 to 20000. The default is **2000**.
	max-suppress-time	(OPTIONAL) Enter the maximum number of minutes a route can be suppressed. The default is four times the half-life value. The range is 1 to 255. The default is **60 minutes**.
	route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route map. Only match commands in the configured route map are supported.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information If you enter `bgp dampening`, the default values for *`half-life`*, *`reuse`*, *`suppress`*, and *`max-suppress-time`* are applied. The parameters are position-dependent; therefore, if you configure one parameter, you must configure the parameters in the order they appear in the command.

Related Commands show ip bgp dampened-paths – views the BGP paths.

bgp default local-preference

Change the default local preference value for routes exchanged between internal BGP peers.

C9000 Series

Syntax `bgp default local-preference` *`value`*

To return to the default value, use the `no bgp default local-preference` command.

Parameters

value	Enter a number to assign to routes as the degree of preference for those routes. When routes are compared, the higher the degree of preference or local preference value, the more the route is preferred. The range is 0 to 4294967295. The default is **100**.

Defaults **100**

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information The `bgp default local-preference` command setting is applied by all routers within the AS.

bgp enforce-first-as

Disable (or enable) enforce-first-as check for updates received from EBGP peers.

C9000 Series

Syntax `bgp enforce-first-as`

To turn off the default, use the `no bgp enforce-first-as` command.

Defaults Enabled.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information This is enabled by default, that is for all updates received from EBGP peers, BGP ensures that the first AS of the first AS segment is always the AS of the peer. If not, the update is dropped and a counter is incremented. Use the `show ip bgp neighbors` command to view the "failed enforce-first-as check" counter.

If you disable enforce-first-as, you can view it using the `show ip protocols` command.

Related Commands

- show ip bgp neighbors – views the information exchanged by BGP neighbors.
- show ip protocols – views information on routing protocols.

bgp fast-external-fallover

Enable the fast external failover feature, which immediately resets the BGP session if a link to a directly connected external peer fails.

C9000 Series

Syntax

`bgp fast-external-fallover`

To disable fast external fallover, use the `no bgp fast-external-fallover` command.

Defaults

Enabled.

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

The `bgp fast-external-fallover` command appears in the `show config` command output.

bgp four-octet-as-support

Enable 4-byte support for the BGP process.

C9000 Series

Syntax

`bgp four-octet-as-support`

To disable fast external fallover, use the `no bgp four-octet-as-support` command.

Defaults

Disabled (supports 2-Byte format).

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced

Usage Information

Routers supporting 4-Byte ASNs advertise that function in the OPEN message. The behavior of a 4-Byte router is slightly different depending on whether it is speaking to a 2-Byte router or a 4-Byte router.

When creating Confederations, all the routers in the Confederation must be 4– or 2–byte identified routers. You cannot mix them.

Where the 2-Byte format is 1-65535, the 4-Byte format is 1-4294967295. Both formats are accepted, and the advertisements will reflect the entered format.

For more information about using the 2– or 4-Byte format, refer to the *Dell Networking OS Configuration Guide*.

bgp graceful-restart

Enable graceful restart on a BGP neighbor, a BGP node, or designate a local router to support graceful restart as a receiver only.

C9000 Series

Syntax

`bgp graceful-restart [restart-time seconds] [stale-path-time seconds] [role receiver-only]`

To return to the default, use the `no bgp graceful-restart` command.

Parameters

neighbor *ip-address* **|** *peer-group-name*	Enter the keyword `neighbor` followed by one of the options listed below: • *ip-address* of the neighbor in IP address format of the neighbor. • *peer-group-name* of the neighbor peer group.
restart-time *seconds*	Enter the keywords `restart-time` followed by the maximum number of seconds needed to restart and bring up all peers. The range is 1 to 3600 seconds. The default is **120 seconds**.
stale-path-time *seconds*	Enter the keywords `stale-path-time` followed by the maximum number of seconds to wait before restarting a peer's stale paths. The default is **360 seconds**.
role receiver-only	Enter the keywords `role receiver-only` to designate the local router to support graceful restart as a receiver only.

Defaults

As above.

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

This feature is advertised to BGP neighbors through a capability advertisement. In Receiver Only mode, BGP saves the advertised routes of peers that support this capability when they restart.

bgp log-neighbor-changes

Enable logging of BGP neighbor resets.

C9000 Series

Syntax

`bgp log-neighbor-changes`

To disable logging, use the `no bgp log-neighbor-changes` command.

Defaults

Enabled.

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

The `bgp log-neighbor-changes` command appears in the `show config` command output.

Related Commands

show config – views the current configuration.

bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems.

C9000 Series

Syntax

`bgp non-deterministic-med`

To return to the default, use the `no bgp non-deterministic-med` command.

Defaults

Disabled (that is, paths/routes for the same destination but from different ASs do not have their MEDs compared).

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

In non-deterministic mode, paths are compared in the order in which they arrive. This method can lead to the system choosing different best paths from a set of paths, depending on the order in which they are received from the neighbors because MED may or may not get compared between adjacent paths. In Deterministic mode (`no bgp non-deterministic-med`), the system compares MED between adjacent paths within an AS group because all paths in the AS group are from the same AS.

When you change the path selection from deterministic to non-deterministic, the path selection for existing paths remains deterministic until you enter the `clear ip bgp` command to clear existing paths.

bgp recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

C9000 Series

Syntax

`bgp recursive-bgp-next-hop`

To disable next-hop resolution, use the `no bgp recursive-bgp-next-hop` command.

Defaults

Enabled.

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

This command is a *knob* to disable BGP next-hop resolution via BGP learned routes. During the next-hop resolution, only the first route that the next-hop resolves through is verified for the route's protocol source and is checked if the route is learned from BGP or not.

The `clear ip bgp` command is required for this command to take effect and to keep the BGP database consistent. Execute the `clear ip bgp` command right after executing this command.

Related Commands

clear ip bgp

bgp regex-eval-optz-disable

Disables the Regex Performance engine that optimizes complex regular expression with BGP.

C9000 Series

Syntax

`bgp regex-eval-optz-disable`

To re-enable optimization engine, use the `no bgp regex-eval-optz-disable` command.

Defaults Enabled.

Command Modes ROUTER BGP (conf-router_bgp)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced

Usage Information BGP uses regular expressions (regex) to filter route information. In particular, the use of regular expressions to filter routes based on AS-PATHs and communities is quite common. In a large scale configuration, filtering millions of routes based on regular expressions can be quite CPU intensive, as a regular expression evaluation involves generation and evaluation of complex finite state machines.

BGP policies, containing regular expressions to match as-path and communities, tend to use a lot of CPU processing time, which in turn affects the BGP routing convergence. Additionally, the `show bgp` commands, which are filtered through regular expressions, use up CPU cycles particularly with large databases. The regex engine performance enhancement feature optimizes the CPU usage by caching and reusing regular expression evaluation results. This caching and reuse may be at the expensive of RP1 processor memory.

Related Commands show ip protocols – views information on all enabled and active routing protocols.

bgp router-id

Assign a user-given ID to a BGP router.

C9000 Series

Syntax `bgp router-id` *`ip-address`*

To delete a user-assigned IP address, use the `no bgp router-id` command.

Parameters

ip-address	Enter an IP address in dotted decimal format to reset only that BGP neighbor.

Defaults The router ID is the highest IP address of the Loopback interface or, if you do not configure Loopback interfaces, the highest IP address of a physical interface on the router.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.4.1.0	Introduced

Usage Information Peering sessions are reset when you change the router ID of a BGP router.

bgp soft-reconfig-backup

To avoid the peer from resending messages, use this command *only* when route-refresh is *not* negotiated.

C9000 Series

Syntax `bgp soft-reconfig-backup`

To return to the default setting, use the `no bgp soft-reconfig-backup` command.

Defaults **Off**

Command Modes ROUTER BGP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for IPv6.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.2.1.0	Introduced.

Usage Information When you enable soft-reconfiguration for a neighbor and you execute the `clear ip bgp soft in` command, the update database stored in the router is replayed and updates are re-evaluated. With this command, the replay and update process is triggered only if route-refresh request is not negotiated with the peer. If the request is indeed negotiated (after executing the `clear ip bgp soft in` command), BGP sends a route-refresh request to the neighbor and receives all of the peer's updates.

Related Commands clear ip bgp — activates inbound policies without resetting the BGP TCP session.

capture bgp-pdu max-buffer-size

Set the size of the BGP packet capture buffer. This buffer size pertains to both IPv4 and IPv6 addresses.

C9000 Series

Syntax `capture bgp-pdu max-buffer-size 100-102400000`

Parameters

100-102400000	Enter a size for the capture buffer.

Defaults **40960000 bytes**

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced

Related Commands

- show capture bgp-pdu neighbor – configures a route reflector and clients.
- capture bgp-pdu neighbor – enables capture of an IPv4 BGP neighbor packet.

capture bgp-pdu neighbor (ipv6)

Enable capture of an IPv6 BGP neighbor packet.

C9000 Series

Syntax `capture bgp-pdu neighbor ipv6-address direction {both | rx | tx}`

To disable capture of the IPv6 BGP neighbor packet, use the `no capture bgp-pdu neighbor ipv6-address` command.

Parameters

ipv6-address	Enter the IPv6 address of the target BGP neighbor.
direction {both | rx | tx}	Enter the keyword `direction` and a direction— either `rx` for inbound, `tx` for outbound, or `both`.

Defaults Not configured.

Command Modes

- EXEC

- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced

Related Commands

- clear ip bgp – enables route reflection between route reflector and clients.
- show capture bgp-pdu neighbor – configures a route reflector and clients.
- capture bgp-pdu neighbor – enables capture of an IPv4 BGP neighbor packet.

clear ip bgp ipv6-address

Reset BGP sessions specific to an IPv6 address. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

C9000 Series

Syntax

```
clear ip bgp ipv6-address [flap-statistics | ipv4 {multicast {flap-statistics | soft {in | out}} | unicast {flap-statistics | soft {in | out}} | ipv6 unicast {flap-statistics | soft {in | out}| soft [in | out]
```

Parameters

ipv6-address	Enter an IPv6 address to reset neighbors belonging to that IP. Used without a qualifier, the keyword resets all neighbors belonging to that IP.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to clear all flap statistics belonging to that AS or a specified address family within that IP.
ipv4	(OPTIONAL) Enter the keyword `ipv4` to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword `ipv6` to select options for that address family.
unicast	(OPTIONAL) Enter the keyword `unicast` to select the unicast option within the selected address family.
multicast	(OPTIONAL) Enter the keyword `multicast` to select the multicast option within the selected address family. Multicast is supported on IPv4 only
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. **NOTE: If you enter `clear ip bgp ip6-address soft`, both inbound and outbound policies are reset.**
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

clear ip bgp * (asterisk)

Reset all BGP sessions in the specified category. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

C9000 Series

Syntax

```
clear ip bgp * [ipv4 multicast soft [in | out] | ipv6 unicast soft [in | out] | soft [in | out]]
```

Parameters

*	Enter an asterisk (*) to reset all BGP sessions.
ipv4 multicast soft [in | out]	(OPTIONAL) This keyword sequence sets options within the a specified IPv4 address family.
ipv6 unicast soft [in | out]	(OPTIONAL) This keyword sequence sets options within the a specified IPv6 address family.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration. **NOTE: If you enter `clear ip bgp ip6-address soft`, both inbound and outbound policies are reset.**
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

clear ip bgp as-number

Reset BGP sessions. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

C9000 Series

Syntax

```
clear ip bgp as-number [flap-statistics | ipv4 {multicast {flap-statistics | soft {in | out}} | unicast {flap-statistics | soft {in | out}} | ipv6 unicast {flap-statistics | soft {in | out}| soft [in | out]
```

Parameters

as-number	Enter an autonomous system (AS) number to reset neighbors belonging to that AS. If used without a qualifier, the keyword resets all neighbors belonging to that AS. The range is 1 to 65535.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to clear all flap statistics belonging to that AS or a specified address family within that AS.
ipv4	(OPTIONAL) Enter the keyword `ipv4` to select options for that address family.
ipv6	(OPTIONAL) Enter the keyword `ipv6` to select options for that address family.
unicast	(OPTIONAL) Enter the keyword `unicast` to select the unicast option within the selected address family.
multicast	(OPTIONAL) Enter the keyword `multicast` to select the multicast option within the selected address family. Multicast is supported on IPv4 only.
soft	(OPTIONAL) Enter the keyword `soft` to configure and activate policies without resetting the BGP TCP session, that is, BGP Soft Reconfiguration.
in	(OPTIONAL) Enter the keyword `in` to activate only inbound policies.
out	(OPTIONAL) Enter the keyword `out` to activate only outbound policies.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

clear ip bgp ipv6 dampening

Clear information on route dampening and return suppressed route to active state.

C9000 Series

Syntax

```
clear ip bgp ipv6 unicast dampening [ipv6-address]
```

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information After you enter this command, the software deletes history routes and returns suppressed routes to active state.

clear ip bgp ipv6 flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

C9000 Series

Syntax `clear ip bgp ipv6 unicast flap-statistics [`*`ipv6-address`*` | filter-list `*`as-path-name`*` | regexp `*`regular-expression`*`]`

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
filter-list *as-path-name*	(OPTIONAL) Enter the keywords `filter-list` followed by the name of a configured AS-PATH list.
regexp *regular-expression*	(OPTIONAL) Enter the keyword `regexp` followed by regular expressions. Use one or a combination of the following: `.` (period) matches on any single character, including white space. `*` (asterisk) matches on sequences in a pattern (zero or more sequences). + (plus sign) matches on sequences in a pattern (one or more sequences). ? (question mark) matches sequences in a pattern (0 or 1 sequences). `[ ]` (brackets) matches a range of single-character patterns. ^ (caret) matches the beginning of the input string. (If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.) $ (dollar sign) matches the end of the output string.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information If you enter `clear ip bgp flap-statistics` without any parameters, all statistics are cleared.

Related Commands show ip bgp ipv6 unicast flap-statistics – views BGP flap statistics.

clear ip bgp ipv6 unicast

Reset MBGP sessions.

C9000 Series

Syntax `clear ip bgp ipv6 unicast * ipv6-address prefix-length [dampening | flap-statistics] peer-group]`

Parameters

*	Enter the character * to clear all peers.
ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
dampening	(OPTIONAL) Enter the keyword `dampening` to clear route flap dampening information.
flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to reset the flap statistics on all prefixes from that neighbor.
peer-group	(OPTIONAL) Enter the keywords `peer-group` to clear all members of a peer-group.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced

clear ip bgp ipv6 unicast dampening

Clear information on route dampening.

C9000 Series

Syntax `clear ip bgp dampening ipv6 unicast [network network-mask]`

Parameters

network	(OPTIONAL) Enter the IPv6 network address in x:x:x:x::x format.
network-mask	If you enter the network address, then enter the network mask, from 0 to 128.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced

clear ip bgp ipv6 unicast flap-statistics

Clear BGP flap statistics, which includes number of flaps and the time of the last flap.

C9000 Series

Syntax `clear ip bgp ipv6 unicast flap-statistics [network | filter-list list |regexp regexp]`

Parameters

network	(OPTIONAL) Enter the IPv6 network address in x:x:x:x::x format to clear flap statistics.
filter-list *list*	(OPTIONAL) Enter the keywords `filter-list` followed by the name of a configured AS-PATH list A maximum of 16 characters.
regexp *regexp*	(OPTIONAL) Enter the keyword `regexp` followed by regular expressions. Use one or a combination of the following: • `.` (period) matches on any single character, including white space. • `*` (asterisk) matches on sequences in a pattern (zero or more sequences). • `+` (plus sign) matches on sequences in a pattern (one or more sequences). • `?` (question mark) matches sequences in a pattern (0 or 1 sequences). • `[ ]` (brackets) matches a range of single-character patterns. • `^` (caret) matches the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` (dollar sign) matches the end of the output string.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced

debug ip bgp keepalives

Allows you to view information about BGP keepalive messages.

C9000 Series

Syntax `debug ip bgp [ipv6-address | peer-group peer-group-name] keepalives [in | out]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] keepalives [in | out]` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group *peer-group-name*	(OPTIONAL) Enter the keywords `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view only information on inbound keepalive routes.
out	(OPTIONAL) Enter the keyword `out` to view only information on outbound keepalive routes.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

debug ip bgp ipv6 dampening

View information on IPv6 routes being dampened.

C9000 Series

Syntax

`debug ip bgp ipv6 unicast dampening [in | out]`

To disable debugging, use the `no debug ip bgp ipv6 unicast dampening` command.

Parameters

in	(OPTIONAL) Enter the keyword `in` to view only information on inbound dampened routes.
out	(OPTIONAL) Enter the keyword `out` to view only information on outbound dampened routes.

Command Modes

EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

Related Commands

show ip bgp dampened-paths – View BGP dampened routes.

debug ip bgp ipv6 unicast peer-group updates

View information about BGP peer-group updates.

C9000 Series

Syntax

`debug ip bgp ipv6 unicast peer-group` *`peer-group-name`* `updates [in | out]`

To disable debugging, use the `no debug ip bgp ipv6 unicast peer-group` *`peer-group-name`* `updates [in | out]` command.

Parameters

peer-group *peer-group-name*	Enter the keywords `peer-group` followed by the name of the peer-group.
updates	Enter the keyword `updates` to view BGP update information.
in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced

debug ip bgp ipv6 unicast dampening

View information on routes being dampened.

C9000 Series

Syntax `debug ip bgp ipv6 unicast dampening`

To disable debugging, use the `no debug ip bgp ipv6 unicast dampening` command.

Parameters

dampening	Enter the keyword `dampening` to clear route flap dampening information.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced

debug ip bgp ipv6 unicast updates

View information about BGP updates.

C9000 Series

Syntax `debug ip bgp ipv6 unicast` *`ipv6-address prefix-length`* `updates [in | out]`

To disable debugging, use the `no debug ip bgp ipv6 unicast` *`ipv6-address prefix-length`* `updates [in | out]` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
updates	Enter the keyword `updates` to view BGP update information.

	in	(OPTIONAL) Enter the keyword `in` to view only BGP updates received from neighbors.
	out	(OPTIONAL) Enter the keyword `out` to view only BGP updates sent to neighbors.

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced

debug ip bgp notifications

Allows you to view information about BGP notifications received from neighbors.

C9000 Series

Syntax `debug ip bgp [ipv6-address | peer-group peer-group-name] notifications [in | out]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name] notifications [in | out]` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group *peer-group-name*	(OPTIONAL) Enter the keywords `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view BGP notifications received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view BGP notifications sent to neighbors.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

debug ip bgp updates

Allows you to view information about BGP updates.

C9000 Series

Syntax

`debug ip bgp [ipv6-address | peer-group peer-group-name | ipv6 unicast [ipv6-address]] updates [in | out | prefix-list prefix-list-name]`

To disable debugging, use the `no debug ip bgp [ip-address | peer-group peer-group-name | ipv6 unicast [ipv6-address]] updates [in | out]` command.

Parameters

ipv6-address	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group *peer-group-name*	(OPTIONAL) Enter the keywords `peer-group` followed by the name of the peer group.
in	(OPTIONAL) Enter the keyword `in` to view BGP updates received from neighbors.
out	(OPTIONAL) Enter the keyword `out` to view BGP notifications updates sent to neighbors.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information Enter the `no debug ip bgp` command to remove all configured debug commands for BGP.

default-metric

Allows you to change the metrics of redistributed routes to locally originated routes. Use this command with the `redistribute` command.

C9000 Series

Syntax

`default-metric number`

To return to the default setting, use the `no default-metric` command.

Parameters

number	Enter a number as the metric to be assigned to routes from other protocols. The range is 1 to 4294967295.

Defaults 0

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information The `default-metric` command in BGP sets the value of the BGP MULTI_EXIT_DISC (MED) attribute for redistributed routes only.

Related Commands

- bgp always-compare-med – enables comparison of all BGP MED attributes.
- redistribute – redistributes routes from other routing protocols into BGP.

description

Enter a description of the BGP routing protocol.

C9000 Series

Syntax `description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the BGP protocol (80 characters maximum).

Defaults none

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Related Commands router bgp – Enter ROUTER mode on the switch.

distance bgp

Configure three administrative distances for routes.

C9000 Series

Syntax

`distance bgp external-distance internal-distance local-distance`

To return to default values, use the `no distance bgp` command.

Parameters

external-distance	Enter a number to assign to routes learned from a neighbor external to the AS. The range is 1 to 255. The default is **20**.
internal-distance	Enter a number to assign to routes learned from a router within the AS. The range is 1 to 255. The default is **200**.
local-distance	Enter a number to assign to routes learned from networks listed in the `network` command. The range is 1 to 255. The default is **200**.

Defaults

- *external-distance* = **20**
- *internal-distance* = **200**
- *local-distance* = **200**

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

CAUTION: Dell Networking recommends that you do not change the administrative distance of internal routes. Changing the administrative distances may cause routing table inconsistencies.

The higher the administrative distance assigned to a route means that your confidence in that route is low. Routes assigned an administrative distance of 255 are not installed in the routing table.

Routes from confederations are treated as internal BGP routes.

ipv6 prefix-list

Configure an IPv6 prefix list.

C9000 Series

Syntax `ipv6 prefix-list prefix-list name`

Parameters

prefix-list name Enter the name of the prefix list.

NOTE: There is a 140-character limit for prefix list names.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

Related Commands show ipv6 prefix-list — View the selected IPv6 prefix-list.

maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

C9000 Series

Syntax `maximum-paths {ebgp | ibgp} number`

To return to the default values, use the `no maximum-paths` command.

Parameters

ebgp Enter the keyword `ebgp` to enable multipath support for External BGP routes.

ibgp Enter the keyword `ibgp` to enable multipath support for Internal BGP routes

number Enter a number as the maximum number of parallel paths. The range is 1 to 16. The default is **1**.

Defaults 1

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information If you enable this command, use the `clear ip bgp` command to recompute the best path.

neighbor activate

This command allows the specified neighbor/peer group to be enabled for the current AFI/SAFI.

C9000 Series

Syntax `neighbor {ipv6-address | peer-group-name} activate`

To disable, use the `no neighbor {ipv6-address | peer-group-name} activate` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Identify a peer group by name.
activate	Enter the keyword `activate` to enable the identified neighbor or peer group in the new AFI/SAFI.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information By default, when you create a neighbor/peer group configuration in the Router BGP context, it is enabled for the IPv6/Unicast AFI/SAFI. By using activate in the new context, the neighbor/peer group is enabled for AFI/SAFI.

neighbor advertisement-interval

Set the advertisement interval between BGP neighbors or within a BGP peer group.

C9000 Series

Syntax

`neighbor {ipv6-address | peer-group-name} advertisement-interval seconds`

To return to the default value, use the `no neighbor {ipv6-address | peer-group-name} advertisement-interval` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
seconds	Enter a number as the time interval, in seconds, between BGP advertisements. The range is 0 to 600 seconds. The default is **5 seconds** for internal BGP peers and **30 seconds** for external BGP peers.

Defaults

- *seconds* = **5 seconds** (internal peers)
- *seconds* = **30 seconds** (external peers)

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

C9000 Series

Syntax

`neighbor {ip-address | peer-group-name} allowas-in number`

To return to the default value, use the `no neighbor {ip-address | peer-group-name} allowas-in` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
number	Enter a number of times to allow this neighbor ID to use the AS path. The range is 1 to 10.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Related Commands bgp four-octet-as-support – enables 4-Byte support for the BGP process.

neighbor default-originate

Inject the default route to a BGP peer or neighbor.

C9000 Series

Syntax `neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]`

To remove a default route, use the `no neighbor {ipv6-address | peer-group-name} default-originate [route-map map-name]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of a configured route map.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information If you apply a route map to a BGP peer or neighbor with the `neighbor default-originate` command configured, the software does not apply the set filters in the route map to that BGP peer or neighbor.

neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

C9000 Series

Syntax `neighbor {ipv6-address | peer-group-name} description text`

To delete a description, use the `no neighbor {ipv6-address | peer-group-name} description text` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
text	Enter a continuous text string up to 80 characters.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

neighbor distribute-list

Distribute BGP information via an established prefix list.

C9000 Series

Syntax

`neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}`

To delete a neighbor distribution list, use the `no neighbor {ipv6-address | peer-group-name} distribute-list prefix-list-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group.
prefix-list-name	Enter the name of an established prefix list. If you do not configure the prefix list, the default is `permit` (to allow all routes).
in	Enter the keyword `in` to distribute only inbound traffic.
out	Enter the keyword `out` to distribute only outbound traffic.

Defaults

Not configured.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

Other BGP filtering commands include the `neighbor filter-list` and `neighbor route-map` commands.

Related Commands

- neighbor filter-list – assigns a AS-PATH list to a neighbor or peer group.
- neighbor route-map – assigns a route map to a neighbor or peer group.

neighbor ebgp-multihop

Attempt and accept BGP connections to external peers on networks that are not directly connected.

C9000 Series

Syntax

`neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]`

To disallow and disconnect connections, use the `no neighbor {ipv6-address | peer-group-name} ebgp-multihop [ttl]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group.
ttl	(OPTIONAL) Enter the number of hops as the time to live (ttl) value. The range is 1 to 255. The default is **255**.

Defaults

Disabled.

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

To prevent loops, the `neighbor ebgp-multihop` command does not install default routes of the multihop peer. Networks not directly connected are not considered valid for best path selection.

neighbor fall-over

Enable or disable fast fall-over for BGP neighbors.

C9000 Series

Syntax

`neighbor {ipv6-address | peer-group-name} fall-over`

To disable, use the `no neighbor {ipv6-address | peer-group-name} fall-over` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**

	peer-group-name	Enter the name of the peer group.

Defaults Disabled.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information When you enable fall-over, BGP keeps track of IP or IPv6 reachability to the peer remote address and the peer local address. Whenever either address becomes unreachable (for example, no active route exists in the routing table for peer IP or IPv6 destination/local address), BGP brings down the session with the peer.

Related Commands show ip bgp neighbors – displays information on the BGP neighbors.

neighbor filter-list

Configure a BGP filter based on the AS-PATH attribute.

C9000 Series

Syntax `neighbor {ipv6-address | peer-group-name} filter-list as-path-name {in | out}`

To delete a BGP filter, use the `no neighbor {ipv6-address | peer-group-name} filter-list as-path-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to apply the filter to all routers in the peer group.
as-path-name	Enter the name of an established AS-PATH access list. If you do not configure the AS-PATH access list, the default is `permit` (to allow routes). The maximum is 16 characters.
in	Enter the keyword `in` to filter inbound BGP routes.
out	Enter the keyword `out` to filter outbound BGP routes.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.4.1.0	Introduced

neighbor maximum-prefix

Control the number of network prefixes received.

C9000 Series

Syntax

`neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]`

To return to the default values, use the `no neighbor {ipv6-address | peer-group-name} maximum-prefix maximum [threshold] [warning-only]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group.
maximum	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is 1 to 4294967295.
threshold	(OPTIONAL) Enter a number to be used as a percentage of the maximum value. When the number of prefixes reaches this percentage of the maximum value, the software sends a message. The range is 1 to 100 percent. The default is **75**.
warning-only	(OPTIONAL) Enter the keywords `warning-only` to set the router to send a log message when the maximum value is reached. If you do not set this parameter, the router stops peering when the maximum number of prefixes is reached.

Defaults

threshold = **75**

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

If you configure the `neighbor maximum-prefix` command and the neighbor receives more prefixes than allowed by the `neighbor maximum-prefix` command configuration, the neighbor goes down and the `show ip bgp summary` command displays (*prfxd*) in the State/PfxRcd column for that neighbor. The neighbor remains down until you enter the `clear ip bgp` command for the neighbor or the peer group to which the neighbor belongs or you enter the `neighbor shutdown` and `neighbor no shutdown` commands.

Related Commands

show ip bgp summary – displays the current BGP configuration.

neighbor next-hop-self

Allows you to configure the router as the next hop for a BGP neighbor. (This command is used for IBGP).

C9000 Series

Syntax

`neighbor {ipv6-address | peer-group-name} next-hop-self [all]`

To return to the default setting, use the `no neighbor {ipv6-address | peer-group-name} next-hop-self [all]` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	(OPTIONAL) Enter the name of the peer group.
all	Specifies that the route reflector is the next hop for both iBGP and eBGP-learned routes.

Defaults

Disabled.

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.10(0.0)	Introduced the `all` keyword on the S4810, S4820, S4048–ON, S3048–ON, S3100 series, S6010–ON, S4040T-ON, S5000, S6000, S6000–ON, S6100–ON, Z9100–ON, and Z9500.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

If you configure the `set ipv6 next-hop` command in ROUTE-MAP mode, its configuration takes precedence over the `neighbor next-hop-self` command.

If you do not use the `all` keyword, the next hop of only eBGP-learned routes is updated by the route reflector. If you use the `all` keyword, the next hop of both eBGP- and iBGP-learned routes are updated by the route reflector.

neighbor peer-group (assigning peers)

Allows you to assign one peer to a existing peer group.

C9000 Series

Syntax

`neighbor ipv6-address peer-group peer-group-name`

To delete a peer from a peer group, use the `no neighbor ipv6-address peer-group peer-group-name` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group *peer-group-name*	Enter the keywords `peer-group` followed by the name of a configured peer group. The maximum is 16 characters.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

You can assign up to 64 peers to one peer group.

When you add a peer to a peer group, it inherits all the peer group's configured parameters. A peer cannot become part of a peer group if any of the following commands are configured on the peer:

- neighbor advertisement-interval
- neighbor distribute-list
- neighbor route-map
- neighbor route-reflector-client
- neighbor send-community

A neighbor may keep its configuration after it was added to a peer group if the neighbor's configuration is more specific than the peer group's, and the neighbor's configuration does not affect outgoing updates.

A peer group must exist before you add a peer to it. If the peer group is disabled (shutdown), the peers within the group are also disabled (shutdown).

Related Commands

- clear ip bgp – resets BGP sessions.
- neighbor peer-group (creating group) – creates a peer group.
- show ip bgp peer-group – view BGP peers.
- show ip bgp neighborsshow ip bgp neighbors View BGP neighbors configurations.

neighbor peer-group (creating group)

Allows you to create a peer group and assign it a name.

C9000 Series

Syntax

`neighbor` *`peer-group-name`* `peer-group`

To delete a peer group, use the `no neighbor` *`peer-group-name`* `peer-group` command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

When a peer group is created, it is disabled (shut mode).

Related Commands

- neighbor peer-group (assigning peers) – assigns routers to a peer group.
- neighbor remote-as – assigns an indirectly connected AS to a neighbor or peer group.
- neighbor shutdown – disables a peer or peer group.

neighbor peer-group passive

Enable passive peering on a BGP peer group, that is, the peer group does not send an OPEN message, but responds to one.

C9000 Series

Syntax

`neighbor` *`peer-group-name`* `peer-group passive`

To delete a passive peer-group, use the `no neighbor` *`peer-group-name`* `peer-group passive` command.

Parameters

peer-group-name	Enter a text string up to 16 characters long as the name of the peer group.

Defaults

Not configured.

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information After you configure a peer group as passive, you must assign it a subnet using the `neighbor subnet` command.

Related Commands neighbor subnet – assigns a subnet to a dynamically-configured BGP neighbor.

neighbor remote-as

Create and specify the remote peer to the BGP neighbor.

C9000 Series

Syntax `neighbor {ipv6-address | peer-group-name} remote-as number`

To delete a remote AS entry, use the `no neighbor {ipv6-address | peer-group-name} remote-as number` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
number	Enter a number of the AS. The range is 1 to 65535.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information If the number parameter is the same as the AS number used in the `router bgp` command, the remote AS entry in the neighbor is considered an internal BGP peer entry.

This command creates a peer and the newly created peer is disabled (shutdown).

Related Commands router bgp – Enter ROUTER BGP mode and configure routes in an AS.

neighbor remove-private-as

Remove private AS numbers from the AS-PATH of outgoing updates.

C9000 Series

Syntax

`neighbor {ipv6-address | peer-group-name} remove-private-as`

To return to the default, use the `no neighbor {ipv6-address | peer-group-name} remove-private-as` command.

Parameters

ipv6-address Enter the IPv6 address in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

peer-group-name Enter the name of the peer group to remove the private AS numbers.

Defaults

Disabled (that is, private AS number are not removed).

Command Modes

ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

Applies to EBGP neighbors only.

If the AS-PATH contains both public and private AS number or contains AS numbers of an EBGP neighbor, the private AS numbers are not removed.

If a confederation contains private AS numbers in its AS-PATH, the software removes the private AS numbers only if they follow the confederation numbers in the AS path.

Private AS numbers are 64512 to 65535.

neighbor route-map

Apply an established route map to either incoming or outbound routes of a BGP neighbor or peer group.

C9000 Series

Syntax

`neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}`

To remove the route map, use the `no neighbor {ipv6-address | peer-group-name} route-map map-name {in | out}` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group.
map-name	Enter the name of an established route map. If you do not configure the Route map, the default is `deny` (to drop all routes).
in	Enter the keyword `in` to filter inbound routes.
out	Enter the keyword `out` to filter outbound routes.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information When you apply a route map to outbound routes, only routes that match at least one section of the route map are permitted.

If you identify a peer group by name, the peers in that peer group inherit the characteristics in the Route map used in this command. If you identify a peer by IP address, the Route map overwrites either the inbound or outbound policies on that peer.

neighbor route-reflector-client

Configure a neighbor as a member of a route reflector cluster.

C9000 Series

Syntax `neighbor {ipv6-address | peer-group-name} route-reflector-client`

To indicate that the neighbor is not a route reflector client or to delete a route reflector configuration, use the `no neighbor {ipv6-address | peer-group-name} route-reflector-client` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**

	peer-group-name	Enter the name of the peer group. All routers in the peer group receive routes from a route reflector.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information The first time you enter this command it configures the neighbor as a route reflector and members of the route-reflector cluster. Internal BGP (IBGP) speakers do not need to be fully meshed if you configure a route reflector.

When all clients of a route reflector are disabled, the neighbor is no longer a route reflector.

neighbor send-community

Send a COMMUNITY attribute to a BGP neighbor or peer group. A COMMUNITY attribute indicates that all routes with that attribute belong to the same community grouping.

C9000 Series

Syntax `neighbor {ipv6-address | peer-group-name} send-community`

To disable sending a COMMUNITY attribute, use the `no neighbor {ipv6-address | peer-group-name} send-community` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.

Defaults Not configured and COMMUNITY attributes are not sent to neighbors.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

neighbor soft-reconfiguration inbound

Enable a BGP soft-reconfiguration and start storing updates for inbound IPv6 unicast routes.

C9000 Series

Syntax

```
neighbor {ipv4-address | ipv6-address | peer-group-name} soft-reconfiguration inbound
```

Parameters

ipv4-address | *ipv6-address*	Enter the IP address of the neighbor for which you want to start storing inbound routing updates.
peer-group-name	Enter the name of the peer group for which you want to start storing inbound routing updates.

Defaults

Disabled.

Command Modes

ROUTER BGPv6 ADDRESS FAMILY (conf-router_bgpv6_af)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.4.1.0	Added support for IPv4 multicast and IPv4 unicast address families.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Introduced on the S4810.
7.7.1.0	Introduced on the C-Series.
7.4.1.0	Introduced

Usage Information

This command enables soft-reconfiguration for the specified BGP neighbor. BGP stores all updates for inbound IPv6 unicast routes the neighbor receives but does not reset the peer-session.

CAUTION: Inbound update storage is a memory-intensive operation. The entire BGP update database from the neighbor is stored in memory regardless of the inbound policy results applied on the neighbor.

neighbor subnet

Enable passive peering so that the members of the peer group are dynamic.

C9000 Series

Syntax

`neighbor` *peer-group-name* `subnet` *subnet-number mask*

To remove passive peering, use the `no neighbor` *peer-group-name* `subnet` *subnet-number mask* command.

Parameters

subnet-number	Enter a subnet number in dotted decimal format (A.B.C.D.) as the allowable range of addresses included in the peer group. To allow all addresses, enter 0::0/0.
mask	Enter a prefix mask in / prefix-length format (/x).

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

neighbor shutdown

Disable a BGP neighbor or peer group.

C9000 Series

Syntax

`neighbor {`*ipv6-address* `|` *peer-group-name*`} shutdown`

To enable a disabled neighbor or peer group, use the `no neighbor {`*ipv6-address* `|` *peer-group-name*`} shutdown` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to disable or enable all routers within the peer group.

Defaults Enabled (that is, BGP neighbors and peer groups are disabled.)

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

Peers that are enabled within a peer group are disabled when their peer group is disabled.

The `neighbor shutdown` command terminates all BGP sessions on the BGP neighbor or BGP peer group. Use this command with caution as it terminates the specified BGP sessions. When a neighbor or peer group is shutdown, use the `show ip bgp summary` command to confirm its status.

Related Commands

- show ip bgp summary – displays the current BGP configuration.
- show ip bgp neighbors – displays the current BGP neighbors.

neighbor timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

C9000 Series

Syntax

`neighbor {`*`ipv6-address | peer-group-name`*`} timers `*`keepalive holdtime`*

To return to the default values, use the `no neighbor {`*`ipv6-address | peer-group-name`*`} timers` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to set the timers for all routers within the peer group.
keepalive	Enter a number for the time interval, in seconds, between keepalive messages sent to the neighbor routers. The range is 1 to 65535. The default is **60 seconds**.
holdtime	Enter a number for the time interval, in seconds, between the last keepalive message and declaring the router dead. The range is 3 to 65535. The default is **180 seconds**.

Defaults

- *keepalive* = **60 seconds**
- *holdtime* = **180 seconds**

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

Timer values configured with the `neighbor timers` command override the timer values configured with the `timers bgp` command.

When two neighbors, configured with different *keepalive* and *holdtime* values, negotiate for new values, the resulting values are as follows:

- the lower of the *holdtime* values is the new *holdtime* value, and
- whichever is the lower value; one-third of the new *holdtime* value, or the configured *keepalive* value is the new keepalive value.

neighbor update-source

Enable the software to use Loopback interfaces for TCP connections for BGP sessions.

C9000 Series

Syntax

`neighbor {`*ipv6-address* | *peer-group-name*`} update-source loopback` *interface*

To use the closest interface, use the `no neighbor {`*ipv6-address* | *peer-group-name*`} update-source loopback` *interface* command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
loopback *interface*	Enter the keyword `loopback` followed by a number of the loopback interface. The range is 0 to 16383.

Defaults Not configured.

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information Loopback interfaces are up constantly and the BGP session may need one interface constantly up to stabilize the session. The `neighbor update-source` command is not necessary for directly connected internal BGP sessions.

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

C9000 Series

Syntax `neighbor {ipv6-address | peer-group-name} weight weight`

To remove a weight value, use the `no neighbor {ipv6-address | peer-group-name} weight weight` command.

Parameters

ipv6-address	Enter the IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
peer-group-name	Enter the name of the peer group to disable all routers within the peer group.
weight	Enter a number as the weight. The range is 0 to 65535. The default is **0**.

Defaults **0**

Command Modes ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information In the software's best path selection process, the path with the highest weight value is preferred.

NOTE: Reset the neighbor connection (the `clear ip bgp *` command) to apply the weight to the connection and recompute the best path.

neighbor X:X:X::X password

Enable TCP MD5 Authentication for an IPv6 BGP peer session.

C9000 Series

Syntax `neighbor x:x:x::x password {7 <encrypt-pass>|<clear-pass>`

To return to the default setting, use the `no neighbor x:x:x::x password` command.

Parameters

encrypt-pass	Enter the encrypted password.
clear-pass	Enter the clear text password.

Defaults Disabled.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced

Usage Information The TCP session is authentication and hence prevents the data from being compromised.

network

Specify the networks for the BGP process and enter them in the BGP routing table.

C9000 Series

Syntax `network ipv6-address prefix-length [route-map map-name]`

To remove a network, use the `no network ip-address mask [route-map map-name]` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
mask	Enter the mask of the IP address in the slash prefix length format (for example, /24). The mask appears in command outputs in dotted decimal format (A.B.C.D).
route-map *map-name*	(OPTIONAL) Enter the keywords *route-map* followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is `deny` (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information The software resolves the network address configured by the `network` command with the routes in the main routing table to ensure that the networks are reachable via non-BGP routes and non-default routes.

Related Commands redistribute – redistributes routes into BGP.

network backdoor

Specify this IGP route as the preferred route.

C9000 Series

Syntax `network ipv6-address prefix-length backdoor`

To remove a network, use the `no network ipv6-address prefix-length backdoor` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The r range is /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information Though the software does not generate a route due to backdoor config, there is an option for injecting/ sourcing a local route in presence of network backdoor config on a learned route.

redistribute

Redistribute routes into BGP.

C9000 Series

Syntax `redistribute {connected | static} [route-map map-name]`

To disable redistribution, use the `no redistribution [connected | static] [route-map map-name]` command.

Parameters

connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If the route map is not configured, the default is `deny` (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced

Usage Information If you do not configure the `default-metric` command in addition to the `redistribute` command, or there is no route map to set the metric, the metric for redistributed static and connected is "0".

To redistribute the default route (0::0/0), configure the `neighbor default-originate` command.

Related Commands neighbor default-originate – injects the default route.

redistribute ospf

Redistribute OSPFv3 routes into BGP.

C9000 Series

Syntax `redistribute ospf process-id [[match external {1 | 2}] [match internal]] [route-map map-name]`

To stop redistribution of OSPF routes, use the `no redistribute ospf process-id` command.

Parameters

process-id	Enter the number of the OSPFv3 process. The range is 1 to 65535.

match external {1 | 2}	(OPTIONAL) Enter the keywords `match external` to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
match internal	(OPTIONAL) Enter the keywords `match internal` to redistribute OSPFv3 internal routes only.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` followed by the name of an established route map. Only the following ROUTE-MAP mode commands are supported: • match ipv6 address • match ipv6 next-hop • match ipv6 route-source • set ipv6 next-hop If you do not configure the route map, the default is `deny` (to drop all routes).

Defaults Not configured.

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information When you enter the `redistribute ospf process-id` command without any other parameters, the software redistributes all OSPF internal routes, external type 1 routes, and external type 2 routes.

router bgp

Enter ROUTER BGP mode to configure and enable BGP.

C9000 Series

Syntax `router bgp` *as-number*

To disable BGP, use the `no router bgp` *as-number* command.

Parameters

process-id	Enter the number of the OSPFv3 process. The range is 1 to 65535.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv6 address.

C9000 Series

Syntax `show capture bgp-pdu neighbor ipv6-address`

Parameters

ipv6-address	Enter the IPv6 address (X:X:X:X::X) of a BGP neighbor.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced

Related Commands

- capture bgp-pdu neighbor – enables capture of an IPv6 BGP neighbor packet.
- clear ip bgp – specifies a size for the capture buffer.

show config

View the current ROUTER BGP configuration.

C9000 Series

Syntax `show config`

Command Modes ROUTER BGPV6-ADDRESS FAMILY

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Example

```
Dell(conf-router_bgp)#show conf
!
router bgp 18508
  neighbor RR-CLIENT peer-group
  neighbor RR-CLIENT remote-as 18508
  neighbor RR-CLIENT no shutdown
  neighbor RR-CLIENT-PASSIV peer-group passive
  neighbor RR-CLIENT-PASSIV remote-as 18508
  neighbor RR-CLIENT-PASSIV subnet 9000::9:0/120
  neighbor RR-CLIENT-PASSIV no shutdown
  neighbor 1109::33 remote-as 18508
  neighbor 1109::33 update-source Loopback 101
  neighbor 1109::33 no shutdown
  neighbor 2222::220 remote-as 18508
  neighbor 2222::220 route-reflector-client
  neighbor 2222::220 update-source Loopback 100
  neighbor 2222::220 no shutdown
  neighbor 4000::33 remote-as 18508
  neighbor 4000::33 no shutdown
  neighbor 4000::60 remote-as 18508
  neighbor 4000::60 no shutdown
  neighbor 9000::1:2 remote-as 640
  no neighbor 9000::1:2 activate
  neighbor 9000::1:2 no shutdown
!
Dell#
```

show ip bgp next-hop

View all next hops (via learned routes only) with current reachability and flap status. This command only displays one path, even if the next hop is reachable by multiple paths.

C9000 Series

Syntax

```
show ip bgp next-hop [local-routes]
```

Parameters

local-routes	(OPTIONAL) Show next-hop information for local routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Example

```
Dell#show ip bgp next-hop
  Next-hop   Via                 RefCount Cost Flaps Time Elapsed
  9000::5:2  9000::5:2, Te 2/38  2        0    0     00:23:22
  9000::6:2  9000::6:2, Te 2/38  2        0    0     00:23:22
  9000::7:2  9000::7:2, Te 2/38  2        0    0     00:23:22
  9000::8:2  9000::8:2, Te 2/38  2        0    0     00:23:22
```

```
  9000::9:2  9000::9:2, Te 2/38  6000     0    0     00:23:16
  9000::a:2  9000::a:2, Te 2/38  2        0    0     00:23:22
Dell#
```

show ip bgp paths

View all the BGP path attributes in the BGP database.

C9000 Series

Syntax `show ip bgp paths [regexp regular-expression]`

Parameters

regexp *regular-expression*	Enter a regular expression then use one or a combination of the following characters to match: • `.` = (period) any single character (including a white space). • `*` = (asterisk) the sequences in a pattern (0 or more sequences). • `+` = (plus) the sequences in a pattern (1 or more sequences). • `?` = (question mark) sequences in a pattern (either 0 or 1 sequences). You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression. • `[ ]` = (brackets) a range of single-character patterns. • `^` = (caret) the beginning of the input string. If the caret is used at the beginning of a sequence or range, it matches on everything BUT the characters specified. • `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp paths as-path

View all unique AS-PATHs in the BGP database.

C9000 Series

Syntax `show ip bgp paths as-path`

Command Modes

- EXEC

- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

C9000 Series

Syntax `show ip bgp paths community`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp paths extcommunity

View all unique Extended community information in the BGP database.

C9000 Series

Syntax `show ip bgp paths extcommunity`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp regexp

Allows you to view the subset of BGP routing table matching the regular expressions specified.

C9000 Series

Syntax

```
show ip bgp regexp regular-expression [character]
```

Parameters

regular-expression [*character*]

Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (0 or more sequences).
- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

  NOTE: You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.
- `[ ]` = (brackets) a range of single-character patterns.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ipv6 prefix-list

Displays the specified IPv6 prefix list.

C9000 Series

Syntax `show ipv6 prefix-list detail {prefix-list name} | summary`

Parameters

detail	Display a detailed description of the selected IPv6 prefix list.
prefix-list name	Enter the name of the prefix list. **NOTE: There is a 140-character limit for prefix list names.**
summary	Display a summary of RPF routes.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.

Related Commands ipv6 prefix-list — configures an IPv6 prefix-list.

show ip bgp ipv6 unicast

View the current BGP routing table.

C9000 Series

Syntax `show ip bgp ipv6 unicast [network [network-mask] [longer-prefixes]]`

Parameters

network	(OPTIONAL) Enter the network address (in dotted decimal format) of the BGP network to view information only on that network.
network-mask	(OPTIONAL) Enter the network mask (in slash prefix format) of the BGP network address.
longer-prefixes	(OPTIONAL) Enter the keywords *longer-prefixes* to view all routes with a common prefix.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information When you enable the `bgp non-deterministic-med` command, the `show ip bgp` command output for a BGP route does not list the INACTIVE reason.

show ip bgp ipv6 unicast cluster-list

View BGP neighbors in a specific cluster.

C9000 Series

Syntax `show ip bgp ipv6 unicast cluster-list [cluster-id]`

Parameters

cluster-id	(OPTIONAL) Enter the cluster id in dotted decimal format.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp ipv6 unicast community

View information on all routes with Community attributes or view specific BGP community groups.

C9000 Series

Syntax `show ip bgp ipv6 unicast community [community-number] [local-as] [no-export] [no-advertise]`

Parameters

community-number	Enter the community number in AA:NN format where AA is the AS number (2 bytes) and NN is a value specific to that autonomous system. You can specify up to eight community numbers to view information on those community groups.
local-AS	Enter the keywords `local-AS` to view all routes with the COMMUNITY attribute of NO_EXPORT_SUBCONFED. All routes with the NO_EXPORT_SUBCONFED (0xFFFFFF03) community attribute must not be advertised to external BGP peers.
no-advertise	Enter the keywords `no-advertise` to view all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords `no-export` to view all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

show ip bgp ipv6 unicast community-list

View routes that are affected by a specific community list.

C9000

Syntax `show ip bgp ipv6 unicast community-list` *`community-list-name`* `[exact-match]`

Parameters

community-list-name	Enter the name of a configured IP community list.
exact-match	(OPTIONAL) Enter exact-match to display only for an exact match of the communities.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp ipv6 unicast dampened-paths

View BGP routes that are dampened (non-active).

C9000 Series

Syntax `show ip bgp ipv6 unicast dampened-paths`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
7.4.1.0	Introduced

show ip bgp ipv6 unicast detail

Display BGP internal information for IPv6 Unicast address family.

C9000 Series

Syntax `show ip bgp ipv6 unicast detail`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp ipv6 unicast extcommunity-list

View information on all routes with Extended Community attributes.

C9000 Series

Syntax `show ip bgp ipv6 unicast extcommunity-list [list name]`

Parameters

list name	Enter the extended community list name you wish to view.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Usage Information

To view the total number of COMMUNITY attributes found, use the `show ip bgp summary` command. The text line above the route table states the number of COMMUNITY attributes found.

The `show ip bgp community` command without any parameters lists BGP routes with at least one BGP community attribute and the output is the same as for the `show ip bgp` command output.

show ip bgp ipv6 unicast filter-list

View the routes that match the filter lists.

C9000 Series

Syntax `show ip bgp ipv6 unicast filter-list as-path-name`

Parameters

as-path-name	Enter the name of an AS-PATH.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp ipv6 unicast flap-statistics

View flap statistics on BGP routes.

C9000 Series

Syntax

```
show ip bgp ipv6 unicast flap-statistics [ipv6-address prefix-length] [filter-list as-path-name] [regexp regular-expression]
```

Parameters

ipv6-address prefix-length
Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

filter-list *as-path-name*
(OPTIONAL) Enter the keywords `filter-list` followed by the name of a configured AS-PATH ACL.

regexp *regular-expression*
Enter a regular expression then use one or a combination of the following characters to match:

- `.` = (period) any single character (including a white space).
- `*` = (asterisk) the sequences in a pattern (0 or more sequences).
- `+` = (plus) the sequences in a pattern (1 or more sequences).
- `?` = (question mark) sequences in a pattern (either 0 or 1 sequences).

  NOTE: You must enter an escape sequence (CTRL+v) prior to entering the ? regular expression.
- `[ ]` = (brackets) a range of single-character patterns.
- `^` = (caret) the beginning of the input string. If you use the caret at the beginning of a sequence or range, it matches on everything BUT the characters specified.
- `$` = (dollar sign) the end of the output string.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.4.1.0	Introduced

show ip bgp ipv6 unicast inconsistent-as

View routes with inconsistent originating autonomous system (AS) numbers; that is, prefixes that are announced from the same neighbor AS but with a different AS-Path.

C9000 Series

Syntax

```
show ip bgp ipv6 unicast inconsistent-as
```

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

show ip bgp ipv6 unicast neighbors

Allows you to view the information exchanged by BGP neighbors.

C9000 Series

Syntax

```
show ip bgp ipv6 unicast neighbors [ipv6-address prefix-length | ip-address]
[advertised-routes | dampened-routes | detail | flap-statistics | routes]
```

Parameters

ipv6-address prefix-length | ip-address	Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros or enter an IP address in dotted decimal format to reset all prefixes from that neighbor.**
advertised-routes	(OPTIONAL) Enter the keywords `advertised-routes` to view only the routes the neighbor sent.
dampened-routes	(OPTIONAL) Enter the keywords `dampened-routes` to view information on dampened routes from the BGP neighbor.
detail	(OPTIONAL) Enter the keyword `detail` to view neighbor-specific internal information for the IPv6 address family.

	flap-statistics	(OPTIONAL) Enter the keywords `flap-statistics` to view flap statistics on the neighbor's routes.
	routes	(OPTIONAL) Enter the keyword `routes` to view only the neighbor's feasible routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Related Commands show ip bgp – view the current BGP routing table.

show ip bgp ipv6 unicast peer-group

Allows you to view information on the BGP peers in a peer group.

C9000 Series

Syntax `show ip bgp ipv6 unicast peer-group [peer-group-name [summary]]`

Parameters

peer-group-name	(OPTIONAL) Enter the name of a peer group to view information about that peer group only.
detail	(OPTIONAL) Enter the keyword `detail` to view peer-group-specific information for the IPv6 address family.
summary	(OPTIONAL) Enter the keyword `summary` to view status information of the peers in that peer group. The output is the same as that found in show ip bgp summary command

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Example

```
Dell#show ip bgp peer-group

Peer-group RR-CLIENT, remote AS 18508
```

```
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::4:

Peer-group RR-CLIENT-PASSIV, remote AS 18508
  BGP version 4
  Minimum time between advertisement runs is 5 seconds

  For address family: IPv4 Unicast
  BGP neighbor is RR-CLIENT-PASSIV, peer-group internal,
  Number of peers in this group 1
  Peer-group members (* - outbound optimized):
    9000::9:2*
Dell#
```

show ip bgp ipv6 unicast summary

Allows you to view the status of all BGP connections.

C9000 Series

Syntax `show ip bgp ipv6 unicast summary`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.

Example

```
Dell# show ip bgp summary
BGP router identifier 55.55.55.55, local AS number 18508
BGP table version is 0, main routing table version 0
6 BGP path attribute entrie(s) using 392 bytes of memory
6 BGP AS-PATH entrie(s) using 294 bytes of memory
6 BGP community entrie(s) using 234 bytes of memory

Neighbor   AS     MsgRcvd MsgSent TblVer InQ OutQ Up/Down State/Pfx

1109::33   18508  0       0       0      0    0 never      Active
2222::220  18508  0       0       0      0    0 never      Active
4000::33   18508  0       0       0      0    0 never      Active
4000::60   18508  0       0       0      0    0 never      Active
9000::4:2  18508  0       0       0      0    0 never      Active
9000::5:2  1      35      32      0      0    0 00:16:42           0
9000::6:2  2      35      32      0      0    0 00:16:39           0
9000::7:2  3      35      32      0      0    0 00:16:41           0
9000::8:2  18508  35      32      0      0    0 00:16:42           0
9000::9:2  18508  44      19      0      0    0 00:16:41           0
9000::a:2  18508  35      32      0      0    0 00:16:43           0
```

```
9000::b:14 18508  29      29      0      0    0 00:13:01          0
Dell#
```

timers bgp

Allows you to adjust the BGP network timers for all neighbors.

C9000 Series

Syntax

`timers bgp` *`keepalive holdtimer`*

To return to the default values, use the `no timers bgp` command.

Parameters

keepalive	Enter the time interval in seconds between which the software sends keepalive messages. The range is 1 to 65535. The default is **60 seconds**.
holdtimer	Enter the time interval in seconds which the software waits since the last keepalive message before declaring a BGP peer dead. The range is 3 to 65535. The default is **180 seconds**.

Defaults

- *`keepalive`* = **60 seconds**
- *`holdtimer`* = **180 seconds**

Command Modes

ROUTER BGP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.2.1.0	Introduced on the E-Series ExaScale.
7.4.1.0	Introduced

Related Commands

neighbor timers – adjusts BGP timers for a specific peer or peer group.

IPv6 MBGP Commands

Multiprotocol BGP (MBGP) is an enhanced BGP that enables the multicast routing policy throughout the internet and connecting multicast topologies between BGP and autonomous systems (AS). MBGP is implemented as per IETF RFC 1858.

show ipv6 mbgproutes

Display the selected IPv6 MBGP route or a summary of all MBGP routes in the table.

C9000 Series

Syntax `show ipv6 mbgproutes ipv6-address prefix-length | summary`

Parameters

ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
summary	Display a summary of RPF routes.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

9

Content Addressable Memory (CAM)

You can use Content Addressable Memory (CAM) commands to configure the amount of memory allocated to CAM memory partitions.

NOTE: Not all CAM commands are supported on all platforms. Be sure to note the platform when looking for a command.

WARNING: If you are using these features for the first time, contact Dell Networking Technical Assistance Center (TAC) for guidance.

Topics:

- CAM Profile Commands
- Unified Forwarding Table Modes

CAM Profile Commands

The CAM profiling feature allows you to partition the CAM to best suit your application. For example:

- Configure more Layer 2 forwarding information base (FIB) entries when the system is deployed as a switch.
- Configure more Layer 3 FIB entries when the system is deployed as a router.
- Configure more access control lists (ACLs) (when IPv6 is not employed).
- Hash multi-protocol label switching (MPLS) packets based on source and destination IP addresses for link aggregation groups (LAGs).
- Hash based on bidirectional flow for LAGs.
- Optimize the virtual local area network (VLAN) ACL Group feature, which permits group VLANs for IP egress ACLs.

Important Points to Remember

- All line cards within a single system must have the same CAM profile (including CAM sub-region configurations); this profile must match the system CAM profile (the profile on the primary route processor module [RPM]).
- The system automatically reconfigures the CAM profile on line cards and the secondary RPM to match the system CAM profile by saving the correct profile on the card and then rebooting it.
- The CAM configuration is applied to the entire system when you use the CONFIGURATION mode commands. Save the running-configuration to affect the change.
- When budgeting your CAM allocations for ACLs and quality of service (QoS) configurations, remember that ACL and QoS rules might consume more than one CAM entry depending on complexity. For example, transmission control protocol (TCP) and user datagram protocol (UDP) rules with `port range` options might require more than one CAM entry.
- After you install a secondary RPM, copy the running-configuration to the startup-configuration so that the new RPM has the correct CAM profile.
- You MUST save your changes and reboot the system for CAM profiling or allocations to take effect.

cam-acl (Configuration)

Select the default CAM allocation settings or reconfigure a new CAM allocation for Layer 2, IPv4, and IPv6 ACLs, Layer 2 and Layer 3 (IPv4) QoS, Layer 2 Protocol Tunneling (L2PT), IP and MAC source address validation for DHCP, Ethernet Connectivity Fault Management (CFM) ACLs, OpenFlow, and Policy-based Routing (PBR).

C9000 Series

Syntax

```
cam-acl {default | l2acl number ipv4acl number ipv6acl number ipv4qos number
l2qos number l2pt number ipmacacl number [vman-qos | vman-dual-qos number]
ecfmacl number [nlbclusteracl number] ipv4pbr number }openflow number | fcoe
number} [iscsioptacl number] [vrfv4acl number]
```

Parameters

default Use the default CAM profile settings and set the CAM as follows:

- L2Acl : 5
- IPV4Acl : 4
- IPV6Acl : 0
- IPV4Qos : 2
- L2Qos : 1
- L2PT : 0
- IpMacAcl : 0
- VmanQos : 0
- VmanDualQos : 0
- EcfmAcl : 0
- nlbclusteracl: 0
- FcoeAcl : 0
- iscsiOptAcl : 0
- ipv4pbr : 0
- Openflow : 0
- fedgovacl : 0
- vrfv4Acl : 0

l2acl *number* Enter the keyword `l2acl` and then the number of l2acl blocks. The range is from 1 to 8.

ipv4acl *number* Enter the keyword `ipv4acl` and then the number of FP blocks for IPv4. The range is from 0 to 8.

ipv6acl *number* Enter the keyword `ipv6acl` and then the number of FP blocks for IPv6. The range is from 0 to 2.

ipv4qos *number* Enter the keyword `ipv4qos` and then the number of FP blocks for IPv4. The range is from 0 to 8.

l2qos *number* Enter the keyword `l2qos` and then the number of FP blocks for l2 qos. The range is from 1to 8.

l2pt *number* Enter the keyword `l2pt` and then the number of FP blocks for l2 protocol tunnelling. The range is from 0 to 1.

Ipmacacl *number*	Enter the keyword `ipmacacl` and then the number of FP blocks for IP and MAC ACL. The range is from 0 to 6.
ecfmacl *number*	Enter the keyword `ecfmacacl` and then the number of FP blocks for ECFM ACL. The range is from 0 to 5.
nlbclusteracl *number*	Enter the keyword `nlbclusteracl` and then the number of FP blocks for nlbcluster ACL. The range is from 0 to 2. By default the value is 0 and it supports 8 NLB arp entries reserved for internal functionality.
Vman-qos|vman-dual-qos *number*	Enter the keyword `evman-qos` and then the number of FP blocks for VMAN QoS. The range is from 0 to 6.
vman-dual-qos *number*	Enter the keyword `vman-dual-qos` and then the number of FP blocks for VMAN dual QoS. The range is from 0 to 4.
Ipv4pbr *number*	Enter the keyword `ipv4pbr` and then the number of FP blocks for ipv4pbr ACL. The range is from 0 to 8.
Openflow *number*	Enter the keyword `openflow` and then the number of FP blocks for open flow (multiples of 4). The range is from 0 to 8.
fcoeacl *number*	Enter the keyword `fcoeacl` and then the number of FP blocks for FCOE ACL. The range is from 0 to 6.
Iscsioptacl *number*	Enter the keyword `iscsioptacl` and then the number of FP blocks for iSCSI optimization ACL. The range is from 0 to 2.
fedgovacl	Enter the keyword `fedgovacl` and then the number of FP blocks for Fed Gov ACL. The range is from 0 to 8.
vrfv4acl *number*	Enter the keyword `vrfv4acl` and then the number of FP blocks for VRF IPv4 ACL. The range is from 0 to 2.
l2acl *number* ipv4acl *number* ipv6acl *number*, ipv4qos *number* l2qos *number*l2pt *number* ipmacacl *number* ecfmacl *number* {nlbclusteracl] [vman-qos | vman-dual-qos *number*] ipv4pbr *number*openflow {4|8} | fcoe *number* [iscsioptacl *number*] [vrfv4acl *number*]	Allocate space to each CAM region. Enter 4 or 8 for the number of OpenFlow FP blocks. • 4: Creates 242 entries for use by the OpenFlow controller (256 total entries minus the 14 entries reserved for internal functionality) • 8: Creates 498 entries for use by the OpenFlow controller (512 total entries minus the 14 entries reserved for internal functionality) The fcoe range is 0–6 groups. Each group has 128 entries; the value given must be an even number. This information is stored in the NVRAM and is effective after rebooting the switch.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added the `nlbcluster ACL` keyword. Introduced on the S6000-ON.
9.4.(0.0)	Added support for PBR and VRF.
9.2(1.0)	Introduced on the Z9500.
9.2(0.2)	Added support for fcoe.
9.1.(0.0)	Added support for OpenFlow.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.2	Clarified block information for the S4810.
8.3.10.0	Introduced on the S4810.
8.3.1.0	Added the keywords `ecfmacl`, `vman-qos`, and `vman-dual-qos`.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.

Usage Information

Save the new CAM settings to the startup-config (`write-mem` or `copy run start`) then reload the system for the new settings to take effect.

The total amount of space allowed is 16 FP Blocks. System flow requires three blocks; these blocks cannot be reallocated. Only 12 number of blocks can be configured by the user .

There can be only one odd number of Blocks in the CLI configuration; the other Blocks must be in factors of 2. For example, a CLI configuration of 5+4+2+1+1 Blocks is not supported; a configuration of 6+4+2+1 Blocks is supported.

The `ipv6acl` allocation must be a factor of 2.

If allocation values are not entered for the CAM regions, the value is 0.

If you enable BMP, to perform a reload on the chassis to upgrade any configuration changes that have changed the NVRAM content, use the command `reload conditional nvram-cfg-change`.

cam-acl-egress

Allocate CAM for egress ACLs.

C9000 Series

Syntax

```
cam-acl-egress default | l2acl number ipv4acl number ipv6acl number}
```

Parameters

default	Reset egress CAM ACL entries to default settings.

l2acl *number* ipv4acl *number* ipv6acl *number*	Allocate space to each CAM region. Enter the CAM profile name then the amount of CAM space to be allotted. The total space allocated must equal 13. The range for ipv4acl is from 1 to 4. The ipv6acl range must be a factor of 2.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

cam-acl-egress-pe

Allocate CAM for egress ACLs on the port extender.

C9000 Series

Syntax `cam-acl-egress-pe {l2acl` *number* `ipv4acl` *number* `ipv6acl` *number*`}`

Parameters

l2acl	Allocates space for the L2 ACL. The default value is 5
ipv4acl	Allocates space for the L3 ACL. The default value is 2.
ipv6acl	Allocates space for the IPv6 L3 ACL. The default value is 2

Defaults None

Command Modes CONFIG

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information Enter the CAM profile name and specify the amount of CAM space. The total space allocated must be equal to 13. The range for `ipv4acl` is from 1 to 4. The `ipv6acl` range must be a factor of 2.

Related Commands **show cam-acl-egress-pe**

cam-acl-pe

Allocate content addressable memory (CAM) for the port extender.

C9000 Series

Syntax

```
cam-acl-pe [default| l2acl number ipv4acl number ipv6acl number ipv4qos number
l2qos number ipmacacl number]
```

Parameters

default	Resets ACL CAM entries to default setting.
l2acl	Allocates space for the L2 ACL. The default value is 5.
ipv4acl	Allocates space for the L3 ACL. The default value is 2.
ipv6acl	Allocates space for the IPv6 L3 ACL. The default value is 2.
ipv4qos	Allocates space for the L3 QoS. The default value is 2.
l2qos	Allocates space for L2 QoS. The default value is 1.
ipmacacl	(Optional) Allocates space for IP and MAC ACLs. The default value is 0.

Defaults None

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command-Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Guidelines Select the CAM allocation for Layer 2, IPv4, and IPv6 ACLs, Layer 2 and Layer 3 (IPv4) QoS, Layer 2 Protocol Tunneling (L2PT), IP and MAC source address validation for DHCP, and Policy-based Routing (PBR). Save the new CAM settings to the startup-config (`write-mem`or `copy run start`) then reload the system for the new settings to take effect. The total amount of space allowed is 12 FP Blocks. System flow requires three blocks; these blocks cannot be reallocated.

The `ipv4acl` profile range is from 1 to 4. When configuring space for`ipv6acl`, the total number of Blocks must equal 13. Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl` profile which is from 0 to 10. The

`ipv6acl` allocation must be a factor of 2 (2, 4, 6, 8, 10). If allocation values are not entered for the CAM regions, the value is 0.

cam-optimization

Optimize CAM utilization for QoS Entries by minimizing require policy-map CAM space.

C9000 Series

Syntax `cam-optimization [qos]`

Parameters

qos	Optimize CAM usage for QoS.

Defaults Disabled.

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.

Usage Information When you enable this command, if a Policy Map containing classification rules (ACL and/or dscp/ ip-precedence rules) is applied to more than one physical interface on the same port pipe, only a single copy of the policy is written (only one FP entry is used). Use this command in Configuration Terminal Batch mode to enable the settings in a dual-homing setup.

NOTE: An ACL itself may still require more that a single FP entry, regardless of the number of interfaces. For more information, refer to the "IP Access Control Lists", "Prefix Lists", and "Route-map" sections in the *Dell Networking OS Configuration Guide*.

cam-threshold

Configure CAM threshold value for sending the syslog message on CAM usage. Configure silence period for stop receiving syslog message on CAM usage.

Syntax

```
cam-threshold threshold {default | threshold-percent} silence-period {default | silence-period-value}
```

Defaults

Enabled

Parameters

threshold default	Enter the keyword `default` for CAM usage threshold for notification of the CAM usage through syslog message. The default threshold value is **90** percent.
threshold *threshold-percent*	Enter the threshold percent for notification of the CAM usage through syslog message. The range is from 1 to 100 percent.
silence-period default	Enter the keyword `default` to set the silence period for receiving syslog message regarding CAM usage for CAM region, slot/portpipe. The default silence period is **0** seconds.
silence-period *silence-period-value*	Enter the silence period for stop receiving syslog message for the respective CAM region, slot/portpipe. The range is from 0 to 65535 seconds.

Command Modes

CONFIGURATION

Supported Modes

Command History

Version	Description
9.13.0.0	Introduced on the MXL, FN IOM, S5000, S4048-ON, S6000, S6000-ON, S3048-ON, S3100 Series, C9010, S4048T-ON, Z9500, Z9100-ON, S6100-ON, S6010-ON.

Usage Information

The `no cam-threshold` command will set the CAM threshold to 90 percent and silence period to 0.

The CAM threshold and silence period configuration is applicable only for Ingress L2, IPv4, IPv6 and Egress L2, IPv4, and IPv6 ACL CAM groups. For other ACL CAM regions, the CAM threshold and silence period is not configurable and the values are fixed to 90 percent and 0 respectively.

Example

```
DellEMC(conf)#cam-threshold threshold 2 silence-period  2
DellEMC(conf)#do show running-config | g cam-threshold
cam-threshold threshold 2 silence-period 2
```

show cam-acl

Display the details of the CAM profiles on the chassis and all stack units.

C9000 Series

Syntax `show cam-acl`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000–ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series.

Usage Information The display reflects the settings implemented with the `cam-acl` command.

Example

show cam-usage

Display the amount of memory space used and available in each CAM partition (including Layer 2 ACL, Layer 3 ACL, and IPv4Flow).

Syntax `show cam-usage [acl | router | switch]`

Parameters

acl	(OPTIONAL) Enter the keyword `acl` to display Layer 2 and Layer 3 ACL CAM usage.
router	(OPTIONAL) Enter the keyword `router` to display Layer 3 CAM usage.
switch	(OPTIONAL) Enter the keyword `switch` to display Layer 2 CAM usage.

Command Modes EXEC

EXEC Privilege

Command History

Version	Description
9.11.0.0	The `show cam-usage` command is updated to display ECMP group count information.
9.5.(0.0)	Introduced on the Z9500.
9.3.(0.0)	Introduced on the S4810, S4820T, Z9000 and MXL.

Usage Information

The following regions must be provided in the `show cam-usage` output:

- L3AclCam
- L2AclCam
- V6AclCam

The following table describes the output fields of the `show cam-usage` command.

Table 2. Output fields of the show cam-usage command

Field	Description
LineCard	Number of the line card that contains information on ACL VLAN groups
Portpipe	The hardware path that packets follow through a system for ACL optimization
CAM-Region	Type of area in the CAM block that is used for ACL VLAN groups
Total CAM space	Total amount of space in the CAM block
Used CAM	Amount of CAM space that is currently in use
Available CAM	Amount of CAM space that is free and remaining to be allocated for ACLs

Example 1: Output of the show cam-usage Command

```
Stackunit|Portpipe| CAM Partition   | Total CAM   |  Used CAM   |Available CAM
========|========|=================|=============|=============|==============
    1   |   0    | IN-L2 ACL       |      1008   |       320   |       688
        |        | IN-L2 FIB       |     32768   |      1132   |     31636
        |        | IN-L3 ACL       |     12288   |         2   |     12286
        |        | IN-L3 ECMP GRP  |      1024   |         0   |      1024
        |        | IN-L3 FIB       |    262141   |        14   |    262127
        |        | IN-L3-SysFlow   |      2878   |        45   |      2833
        |        | IN-L3-TrcList   |      1024   |         0   |      1024
        |        | IN-L3-McastFib  |      9215   |         0   |      9215
        |        | IN-L3-Qos       |      8192   |         0   |      8192
        |        | IN-L3-PBR       |      1024   |         0   |      1024
        |        | IN-V6 ACL       |         0   |         0   |         0
        |        | IN-V6 FIB       |         0   |         0   |         0
        |        | IN-V6-SysFlow   |         0   |         0   |         0
        |        | IN-V6-McastFib  |         0   |         0   |         0
        |        | OUT-L2 ACL      |      1024   |         0   |      1024
        |        | OUT-L3 ACL      |      1024   |         0   |      1024
        |        | OUT-V6 ACL      |         0   |         0   |         0
    1   |   1    | IN-L2 ACL       |       320   |         0   |       320
        |        | IN-L2 FIB       |     32768   |      1136   |     31632
        |        | IN-L3 ACL       |     12288   |         2   |     12286
        |        | IN-L3 FIB       |    262141   |        14   |    262127
```

```
        |        | IN-L3-SysFlow   |      2878   |        44   |      2834
--More--
```

Example 2: Output of the show cam-usage acl Command

```
Dell#show cam-usage acl
Stackunit|Portpipe| CAM Partition   | Total CAM   |  Used CAM   |Available CAM
========|========|=================|=============|=============|============
   11   |   0    | IN-L2 ACL       |      1008   |          0  |      1008
        |        | IN-L3 ACL       |     12288   |          2  |     12286
        |        | OUT-L2 ACL      |      1024   |          2  |      1022
        |        | OUT-L3 ACL      |      1024   |          0  |      1024
        |        | IN-L3 ECMP GRP  |      1024   |          0  |      1024
```

Example 3: Output of the show cam-usage router Command

Example 4: Output of the show cam-usage switch Command

show cam-acl-pe

Display details of global ingress CAM ACL profiles for the port extender.

C9000 Series

Syntax

```
show cam-acl-pe
```

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

The display reflects the settings implemented with the `cam-acl-pe`command.

This command only displays the details of CAM ACL profiles configured globally on the PE. It does not display CAM ACL profiles for each PE.

Example

```
Dell# show cam-acl-pe

-- Port extender Cam ACL --
        Current Settings(in block sizes)
           1 block = 256 entries
L2Acl      :         6
```

```
Ipv4Acl    :          4
Ipv6Acl    :          0
Ipv4Qos    :          2
L2Qos      :          1
IpMacAcl   :          0
```

show cam-acl-egress-pe

Display details of the global egress CAM ACL profiles for the port extender.

C9000 Series

Syntax `show cam-acl-egress-pe`

Defaults None

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information The display reflects the settings implemented with the `cam-acl-egress-pe` command.

This command only displays the details of CAM ACL egress profiles configured globally on the PE. It does not display CAM ACL egress profiles for each PE.

Example

```
Dell# show cam-acl-egress-pe

-- Port extender Egress Cam ACL --
        Current Settings(in block sizes)
           1 block = 256 entries
L2Acl      :          1
Ipv4Acl    :          1
Ipv6Acl    :          2
```

test cam-usage

Verify the CAM space that is available for IPv4 and IPv6 CAM profiles, and particularly to verify if enough CAM space is available for the IPv6 ACLs you use in a policy map.

C9000 Series

Syntax

```
test cam-usage service-policy input policy-map-name linecard {number portset {port-pipe-number} | all}
```

Parameters

input *policy-map-name*	Enter the name of the policy map to verify. Maximum is 32 characters.
linecard *number* portset *port-pipe-number*	Enter a line card and port-pipe number to check CAM usage on specified ports. The range of valid port-pipe numbers is 0 to 3. Enter `linecard all` to verify the CAM space available for all ports on the switch.

Defaults

None

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced.

Usage Information

This command applies to both IPv4 and IPv6 CAM Profiles, but is best used when verifying QoS optimization for IPv6 ACLs.

QoS Optimization for IPv6 ACLs does not impact the CAM usage for applying a policy on a single (or the first of several) interfaces. It is most useful when a policy is applied across multiple interfaces; it can reduce the impact to CAM usage across subsequent interfaces.

The following describes the `test cam-usage` command shown in the following example.

Term	Explanation
Linecard	Lists the line cards that are checked. Entering `all` displays the status for line cards in the chassis.
Portpipe	Lists the port pipes (port sets) that are checked. Entering `all` displays the status for all line cards and port pipes in the chassis.

Term	Explanation
CAM Partition	Shows the CAM profile of the CAM.
Available CAM	Identifies the amount of CAM space remaining for that profile.
Estimated CAM per Port	Estimates the amount of CAM space the listed policy will require.
Status	Indicates whether or not the policy will be allowed in the CAM.

Example

```
Dell# test cam-usage service-policy input pcam linecard all
linecard |Portpipe|CAM Partition|Available CAM |Estimated CAM per Port|Status
--------------------------------------------------------------------------------
   0     |   0    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   0     |   1    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   0     |   2    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   1     |   0    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   1     |   1    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   1     |   2    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   1     |   3    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   2     |   0    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   2     |   1    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   2     |   2    |    IPv4Flow    |   408  |  1 |  Allowed (408)
   2     |   3    |    IPv4Flow    |   408  |  1 |  Allowed (408)
```

Unified Forwarding Table Modes

Unified Forwarding Table (UFT) consolidates the resources of several search tables (Layer 2, Layer 3 Hosts, and Layer 3 Route [Longest Prefix Match — LPM]) into a single flexible resource. Trident 2 supports several UFT modes to extract the forwarding tables, as required. By default, Dell Networking OS initializes the table sizes to UFT mode 2 profile, since it provides a reasonable shared memory for all the tables. The other supported UFT modes are scaled-l3–hosts (UFT mode 3) and scaled-l3–routes (UFT mode 4).

Important Points to Remember

- All line cards/Stack Members within a single system must have the same UFT mode profiles. this profile must match the system UFT mode profile (the profile on the primary route processor module [RPM]/ Master Unit of the Stack).
- The UFT mode configuration is applied to the entire system when you use the CONFIGURATION mode commands. Save the running-configuration to affect the change.
- You MUST save your changes and reboot the system for UFT mode profiling to take effect.

show hardware forwarding-table mode

Display the hardware forwarding table mode in the current boot and in the next boot.

Syntax `show hardware forwarding-table mode`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.7(0.0)	Introduced on the S6000, S6000-ON, and Z9500 switch.

Example

```
Dell#show hardware forwarding-table mode

                     Current Settings            Next Boot Settings
Mode               :  Default                     scaled-l3-hosts
L2 MAC Entries     :  160K                         96K
L3 Host Entries    :  144K                        208K
L3 Route Entries   :   16K                         16K

Dell#
```

Related Commands hardware forwarding-table mode — selects the mode to initialize the maximum scalability size for L2 MAC table or L3 Host table or L3 Route table.

hardware forwarding-table mode

Select a mode to initialize the maximum scalability size for L2 MAC table or L3 Host table or L3 Route table.

Syntax `hardware forwarding-table mode {scaled-l3- hosts | scaled-l3-routes}`

Parameters

scaled-l3-hosts	Enter the keyword `scaled-l3-hosts` to select the forwarding table mode for scaling l3 host entries..
scaled-l3-routes	Enter the keyword `scaled-l3-routes` to select the forwarding table mode for scaling l3 route entries.

Defaults UFT mode 2

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000, S6000-ON, and Z9500 switch..

Usage Information This command takes effect only after reboot.

On the C9010, OpenFlow supports only the scaled-l3-hosts hardware forwarding-table mode (UFT mode 3), providing a unified forwarding table (UFT) of:

- L2 MAC entries: 160K
- L3 host entries: 144K
- L3 route entries: 16K

OpenFlow does not support the scaled-l3-routes forwarding-table mode (UFT mode 4) on the C9010.

Related Commands show hardware forwarding-table mode — displays the hardware forwarding table mode in the current boot and in the next boot.

10

Control Plane Policing (CoPP)

Control plane policing (CoPP) uses access control list (ACL) rules and quality of service (QoS) policies to create filters for a system's control plane. The CoPP filters prevent traffic that is not identified as legitimate from reaching the control plane, and rate-limit traffic to an acceptable level.

On the switch, the control plane has 21 queues (0 to 20) divided into groups of seven queues for the Route Processor, Control Processor, and line-card CPUs as follows:

- Queues 0 to 6 process packets destined to the Control Processor CPU .
- Queues 7 to 13 process packets destined to the Route Processor CPU.
- Queues 14 to 20 process packets destined to the line card CPU.

Topics:

- clear control-traffic protocol
- clear control-traffic queue
- control-plane-cpuqos
- service-policy rate-limit-cpu-queues
- service-policy rate-limit-protocols
- show control-traffic protocol
- show control-traffic queue
- show cpu-queue rate
- show ip protocol-queue-mapping
- show ipv6 protocol-queue-mapping
- show mac protocol-queue-mapping
- show protocol-queue-mapping

clear control-traffic protocol

Clear all per-protocol counters of rate-limited control-plane traffic.

C9000 Series

Syntax

```
clear contol—traffic protocol [all | cp-switch | linecard slot-id portset port-pipe | pe {pe-id stack-unit unit number portset port-pipe ID} [counters]]
```

Parameters

cp-switch	Enter the keyword `cp-switch` to clear counters for rate-limited traffic on the central switch (aggregated CoPP).
all	Enter the keyword `all` to clear counters for all protocol rate-limiting traffic information.
pe *pe-id*	Enter the keyword `pe` and the port extender ID. The PE ID range is from 0 to 255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the stack unit number. The stack-unit range is from 0 to 7.

	portset *port-pipe ID*	Enter the keyword `portset` and the port-pipe ID. The port-pipe ID value is 0.

Defaults Clear per-protocol rate-limiting counters for all control-plane and port-set (port-pipe) traffic.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information To display the per-protocol counters of rate-limited control-plane traffic at the aggregated (switch) or line card and port set level, use the `show control-traffic protocol` command.

clear control-traffic queue

Clear per-queue counters of rate-limited control-plane traffic.

C9000 Series

Syntax `clear contol—traffic queue {all | queue-number} counters`

Parameters

all	Enter the keyword `all` to clear counters for rate-limited traffic on all CPU queues, including Route Processor, Control Processor, and line-card CPUs.
queue-number	Enter the queue number to clear counters for rate-limited traffic on a specified CPU queue. The range of queue-number values is from 0 to 20. The twenty-one control—plane queues are divided into groups of seven queues for the Route Processor, Control Processor, and line-card CPUs as follows: • Queues 0 to 6 process packets destined to the Control Processor CPU . • Queues 7 to 13 process packets destined to the Route Processor CPU. • Queues 14 to 20 process packets destined to the line card CPU.

Defaults Clear per-queue rate-limiting counters for all control-plane and port traffic.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information

To display the per-queue counters of rate-limited control-plane traffic at the aggregated (switch), use the `show control-traffic queue` command.

Example

```
Dell#clear control-traffic queue 2 counters
Dell#
```

control-plane-cpuqos

To manage control-plane traffic, enter control-plane mode and configure the switch.

C9000 Series

Syntax `control-plane-cpuqos`

Defaults Not configured.

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

service-policy rate-limit-cpu-queues

Apply a QoS input policy-map that rate-limits traffic on control-plane queues.

C9000 Series

Syntax `service-policy rate-limit-cpu-queues policy-name`

Parameters

policy-name	Enter the service-policy name, using a string up to 32 characters.

Defaults Not configured.

Command Modes CONTROL-PLANE-CPUQOS

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information Create a policy-map by associating a queue number with the qos-policy.

Create QoS policies prior to enabling this command.

Related Commands qos-policy-input cpu-qos — creates a QoS input-policy map for CoPP.

policy-map-input cpu-qos — creates an input-policy map for CoPP.

service-policy rate-limit-protocols

Apply a QoS input policy-map that rate-limits protocol traffic on the control plane.

C9000 Series

Syntax `service-policy rate-limit-protocols policy-name`

Parameters

policy-name	Enter the service-policy name, using a string up to 32 characters.

Defaults Not configured.

Command Modes CONTROL-PLANE-CPUQOS

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information This command applies the service-policy based on the type of protocol defined in the ACL rules.

Create ACL and QoS policies prior to enabling this command.

If you configure rate-limiting of control protocols on a per-protocol basis and if you modify the rate using the `rate-police` command in QOS-POLICY-IN mode while traffic is being passed, packet drops for the specified protocols may occur if you configure a rate higher than the default rate for a protocol.

Related Commands ip access-list extended cpu-qos — creates an extended IP ACL for CoPP.

mac access-list extended cpu-qos — creates an extended MAC ACL for CoPP.

class-map cpu-qos — creates a QoS class map for CoPP.

qos-policy-input cpu-qos — creates a QoS input-policy map for CoPP.

policy-map-input cpu-qos — creates an input-policy map for CoPP.

show control-traffic protocol

Display per-protocol counters of rate-limited control-plane traffic.

C9000 Series

Syntax `show contol—traffic protocol [cp—switch | linecard` *`slot-id`* `portset` *`port-pipe`* `| pe` *`pe-id`* `stack-unit` *`unit-number`* `portset` *`port-pipe`* `] counters`

Parameters

cp-switch	Enter the keyword `cp-switch` to display counters for rate-limited traffic on the central switch (aggregated CoPP).
linecard *slot-id* **portset** *port-pipe*	Enter the slot ID and port pipe to display counters for rate-limited traffic on a specified line card and port set. The slot ID range is from 0 to 11. The port-pipe ID value is 0.
pe *pe-id*	Enter the keyword `pe` and the port extender ID. Range is from 0 to 255.

stack-unit *unit number*	Enter the keyword `stack-unit` and the stack unit number. Range is from 0 to 7.
portset *port-pipe*	Enter the keyword `portset` and the port-pipe ID. Port pipe ID value is 0.
counters	Enter the keyword `counters` to display the traffic counters.

Defaults None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Usage Information In the `show control-traffic protocol` output, RxBytes displays the number of bytes of control-plane traffic received on which protocol-based rate limiting is applied. TxBytes displays the number of bytes transmitted to a control-plane CPU after protocol-based rate limiting is applied. Drops display the number of bytes of control-plane traffic that have been dropped as a result of protocol-based rate limiting.

The number of RxBytes is calculated as: Drops/<*packet-size*> + TxBytes/<*packet-size* + 4 bytes> = RxBytes (total packets received)

To clear the per-protocol counters of rate-limited control-plane traffic at the aggregated (switch) or line card and port set level, use the `clear control-traffic protocol` command.

Example (PE)

```
Dell#show control-traffic protocol pe 3 stack-unit 0 portset 0 counters
 Protocol                                        RxBytes  TxBytes  Drops
 -------                                         -------  -------  ------
STP/ARP/ICMP(v4/v6)/IGMP/MLD/NTP/FTP/TELNET/SSH  0        0        0
PE CSP/PE-CB LLDP                                131227   131227   0
LLDP/LACP/8021x                                  0        0        0
```

Example

```
Dell#show control-traffic protocol linecard 2 portset 0 counters
Protocol               RxBytes        TxBytes     Drops
-------                -------        -------     -----
STP                    14956278172    403036      14955875136
LLDP                   15029657016    559096      15029097920
PVST                   0              0           0
LACP                   15122824104    556648      15122267456
GVRP                   14988129080    551480      14987577600
ARP RESP/ARP REQ       29604578172    3559868     29601018304
802.1x                 0              0           0
FEFD                   0              0           0
FRRP                   0              0           0
ECFM                   0              0           0
L2PT                   0              0           0
ISIS                   0              0           0
BFD                    0              0           0
BGP                    0              0           0
v6 BGP                 0              0           0
OSPF                   0              0           0
v6 OSPF                0              0           0
RIP                    0              0           0
VRRP                   0              0           0
v6 VRRP                0              0           0
```

```
IGMP                    0               0               0
PIM                     0               0               0
NTP                     0               0               0
MULTICAST CATCH ALL     0               0               0
v6 MULTICAST CATCH ALL  0               0               0
DHCP RELAY/DHCP         0               0               0
v6 ICMP NA/v6 ICMP RA   0               0               0
v6 ICMP NS/v6 ICMP RS   0               0               0
v6 ICMP/ICMP            0               0               0
MLD                     0               0               0
MSDP                    0               0               0
FTP/TELNET/SSH/
L3 LOCAL TERMINATED     0               0               0
L3 UNKNOWN/UNRESOLVED ARP 0             0               0
iSCSI                   0               0               0
FCoE                    0               0               0
SFLOW                   0               0               0
VLT CTRL/VLT IPM PDU    0               0               0
HYPERPULL               0               0               0
OPENFLOW                0               0               0
L2 DST HIT/BROADCAST    0               0               0
VLT TTL1/TRACEFLOW/TTL0/
STATION MOVE/TTL1/IP OPTION/
L3 MTU FAIL/SOURCE MISS  0              0               0
```

Related Command clear control-traffic protocol

show control-traffic queue

Display per-queue counters of rate-limited control-plane traffic.

C9000 Series

Syntax `show contol—traffic queue {all | queue-id` *`queue-number`*`} counters`

Parameters

all	Enter the keyword `all` to display counters for rate-limited traffic on all CPU queues, including Route Processor, Control Processor, and line-card CPUs.
queue-id *queue-number*	Enter the queue number to display counters for rate-limited traffic on a specified CPU queue. For the C9000 Series, the range of queue-number values is from 0 to 20. The twenty-one control–plane queues are divided into groups of seven queues for the Route Processor, Control Processor, and line-card CPUs as follows: C9000 Series • Queues 0 to 6 process packets destined to the Control Processor CPU . • Queues 7 to 13 process packets destined to the Route Processor CPU. • Queues 14 to 20 process packets destined to the line card CPU.

Defaults None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information

In the `show` output, Rx Bytes displays the number of bytes of control-plane traffic received, on which queue-based rate limiting is applied. Tx Counters displays the number of bytes transmitted to a control-plane CPU after queue-based rate limiting is applied. Drop Counters displays the number of bytes of control-plane traffic that have been dropped as a result of queue-based rate limiting.

To clear the per-queue counters of rate-limited control-plane traffic at the aggregated (switch), use the `clear control-traffic queue` command.

Example

```
Dell#show control-traffic queue queue-id 0 counters
Queue       Rx Counter    Tx Counter     Drop counter
-----------------------------------------------------------
Q0        5000        5000        0
Dell#
```

Related Command

clear control-traffic queue

show cpu-queue rate

Display the rates for each control-plane queue.

C9000 Series

Syntax

`show cpu-queue rate [all | queue-id` *`queue-number`* `| range` *`from_queue to_queue`*`]`

Parameters

all	Display the rate for all control-plane queues. The CPU queues range is from 0 to 20.
queue-id *queue-number*	Display the rate for a specified control-plane queue. The CPU queue value range is from 0 to 20.
range *from_queue to_queue*	Display the rate for a range of control-plane queues. The CPU queue value range is from 0 to 20. Separate the *from_queue* value from the *to_queue* value with a space; for example, `show cpu-queue rate range 8 15`.

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information This command displays the currently configured control-plane queue rate at the aggregated switch.

Example: C9000 Series

```
Dell#do sh cpu-queue rate all
 Service-Queue         Rate (kbps)      Burst (kb)
 --------------        -----------      ----------
Q0                        400              1000
Q1                        600              1000
Q2                        600              1000
Q3                        2000             5000
Q4                        300              2000
Q5                        300              2000
Q6                        1200             3000
Q7                        800              1000
Q8                        600              1000
Q9                        600              1000
Q10                       3200             1000
Q11                       2600             6000
Q12                       2300             3000
Q13                       1800             3000
Q14                       1                4000
Q15                       1                100
Q16                       1200             100
Q17                       1200             1000
Q18                       7000             1000
Q19                       800              7000
Q20                       5000             1000
```

```
Dell#show cpu-queue rate queue-id 8
 Service-Queue         Rate (kbps)      Burst (kb)
 --------------        -----------      ----------
Q8                        600              1000

Dell#show cpu-queue rate range 8 12
 Service-Queue         Rate (kbps)      Burst (kb)
 --------------        -----------      ----------
Q8                        600              1000
Q9                        600              1000
Q10                       3200             1000
Q11                       2600             6000
Q12                       2300             3000
```

show ip protocol-queue-mapping

Display the CPU queue mapping for IPv4 protocols.

C9000 Series

Syntax `show ip protocol-queue-mapping` *queue-id*

Defaults Not configured.

Command Modes EXEC Privilege

Usage Information The `show` output displays information on CPU traffic flows for IPv4 protocols, including the ingress queue at which the traffic is queued and the CPU to which protocol traffic is sent with the applied rate limits (configured or default) in kilobits per second (kbps). The egress port queues on CPUs are abbreviated as: RP (Route Processor), CP (Control Processor), and LC (line card).

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show ip protocol-queue-mapping
 Protocol    Src-Port    Dst-Port    TcpFlag  Queue    EgPort      Rate (kbps)
 --------    --------    --------    -------  -----    ------      -----------
TCP (BGP)      any/179     179/any      _        Q13      RP           2500
UDP (DHCP)     67/68       68/67        _        Q6       CP           1200
UDP (DHCP-R)   67          67           _        Q6       CP           1200
TCP (FTP)      any         21           _        Q3       CP           400
ICMP           any         any          _        Q5       CP           300
IGMP           any         any          _        Q12      RP           300
TCP (MSDP)     any/639     639/any      _        Q12      RP           100
UDP (NTP)      any         123          _        Q3       CP           200
OSPF           any         any          _        Q13      RP           2500
PIM            any         any          _        Q12      RP           300
UDP (RIP)      any         520          _        Q13      RP           200
TCP (SSH)      any         22           _        Q3       CP           400
TCP (TELNET)   any         23           _        Q3       CP           400
VRRP           any         any          _        Q13      RP           400
```

show ipv6 protocol-queue-mapping

Display the CPU queue mapping for IPv6 protocols.

C9000 Series

Syntax `show ipv6 protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Usage Information

The `show` output displays information CPU traffic flows for supported IPv6 protocols, including the ingress queue at which the traffic is queued and the CPU to which protocol traffic is sent with the applied rate limits (configured or default) in kilobits per second (kbps). The egress port queues on CPUs are abbreviated as: RP (Route Processor), CP (Control Processor), and LC (line card).

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show ipv6 protocol-queue-mapping

 Protocol   Src-Port   Dst-Port   TcpFlag  Queue   EgPort     Rate (kbps)
 --------   --------   --------   -------  -----   ------     -----------
TCP (BGP)     any/179    179/any      _       Q15     RP          2500
ICMPV6 NA     any        any          _       Q3/Q11  CP/RP       600
ICMPV6 RA     any        any          _       Q3/Q11  CP/RP       600
ICMPV6 NS     any        any          _       Q2/Q10  CP/RP       600
ICMPV6 RS     any        any          _       Q2/Q10  CP/RP       600
ICMPV6        any        any          _       Q5      CP          300
VRRPV6        any        any          _       Q15     RP          400
OSPFV3        any        any          _       Q15     RP          2500
```

show mac protocol-queue-mapping

Display the CPU queue mapping for MAC protocols.

C9000 Series

Syntax `show mac protocol-queue-mapping`

Defaults Not configured.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show mac protocol-queue-mapping
 Protocol     Destination Mac       EtherType   Queue          EgPort     Rate
(kbps)
 --------     ---------------       ---------   -----          ------
-----------
ARP           any                   0x0806      Q1/Q8/Q2/Q9     CP/RP
100
FRRP          01:01:e8:00:00:10/11  any         Q19             LP
300
LACP          01:80:c2:00:00:02     0x8809      Q13             RP
500
LLDP          any                   0x88cc      Q6              CP
500
GVRP          01:80:c2:00:00:21     any         Q12             RP
200
STP           01:80:c2:00:00:00     any         Q13             RP
150
ISIS          01:80:c2:00:00:14/15  any         Q13             RP
500
              09:00:2b:00:00:04/05  any         Q13             RP
500
```

show protocol-queue-mapping

Display the protocol-queue mapping for each configured protocol.

C9000 Series

Syntax `show protocol-queue-mapping [queue-id queue-number]`

Parameters

queue-id *queue-number*	(Optional) Display the protocol-queue mapping for a specified control-plane queue. The range of CPU queue numbers is from 0 to 20.

Defaults Not configured.

Command Modes EXEC Privilege

Usage Information The `show` output displays information on CPU traffic flows for all protocols, including the ingress queue at which the traffic is queued and the CPU to which protocol traffic is sent with the applied rate limits (configured or default) in kilobits per second (kbps). The egress port queues on CPUs are abbreviated as: RP (Route Processor), CP (Control Processor), and LC (line card).

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show protocol-queue-mapping | no-more
Protocol                  Queue        EgPort  CommitRate(kbps) Peak
Rate(kbps) CommitBurst(kb) Peak Burst(kb)
--------                  -----        ------  ---------------  -------------
--------------  ------------
STP                       Q13          RP      150              150
1000             1000
LLDP                      Q6           CP      500              500
1000             1000
PVST                      Q12          RP      200              200
1000             1000
LACP                      Q13          RP      500              500
1000             1000
ARP                       Q1/Q8/Q2/Q9  CP/RP   100              100
800              800
GVRP                      Q12          RP      200              200
1000             1000
FRRP                      Q19          LP      300              300
1000             1000
ECFM                      Q13          RP      150              150
1000             1000
ISIS                      Q13          RP      500              500
3000             3000
L2PT                      Q13          RP      150              150
1000             1000
v6 BGP                    Q13          RP      2500             2500
2000             2000
v6 OSPF                   Q13          RP      2500             2500
2000             2000
v6 VRRP                   Q13          RP      400              400
2000             2000
MLD                       Q12          RP      150              150
500              500
v6 MULTICAST CATCH ALL    Q7           RP      100              100
500              500
IPv6 DHCP                 Q6           CP      1200             1200
2000             2000
v6 RAGUARD                Q16          LP      600              600
1000             1000
v6 ICMP NA                Q2/Q9        CP/RP   600              600
1000             1000
v6 ICMP RA                Q2/Q9        CP/RP   600              600
1000             1000
v6 ICMP NS                Q1/Q8        CP/RP   600              600
1000             1000
v6 ICMP RS                Q1/Q8        CP/RP   600              600
1000             1000
v6 ICMP                   Q4           CP      300              300
2000             2000
BGP                       Q13          RP      2500             2500
2000             2000
OSPF                      Q13          RP      2500             2500
2000             2000
RIP                       Q13          RP      200              200
1000             1000
VRRP                      Q13          RP      400              400
```

```
2000              2000
ICMP                        Q5          CP      300             300
2000              2000
IGMP                        Q12         RP      300             300
2000              2000
PIM                         Q12         RP      300             300
2000              2000
MSDP                        Q12         RP      100             100
2000              2000
BFD                         Q11/Q17     RP/LP   7000            7000
3000              3000
802.1x                      Q6          CP      150             150
1000              1000
iSCSI                       Q7          RP      100             100
500               500
DHCP RELAY                  Q6          CP      1200            1200
2000              2000
DHCP                        Q6          CP      1200            1200
2000              2000
NTP                         Q3          CP      200             200
2000              2000
FTP                         Q3          CP      400             400
3000              3000
TELNET                      Q3          CP      400             400
2000              2000
SSH                         Q3          CP      400             400
2000              2000
VLT GARP                    Q3/Q10      CP/RP   500             500
3000              3000
VLT CTRL - CP CPU           Q3          CP      2000            2000
3000              3000
VLT CTRL - RP CPU           Q10         RP      2000            2000
3000              3000
VLT CTRL - CP & RP CPU      Q3/Q10      CP/RP   2000            2000
3000              3000
VLT CTRL - HA               Q10         RP      2000            2000
3000              3000
VLT CTRL                    Q10         RP      2000            2000
3000              3000
VLT IPM PDU                 Q3/Q10      CP/RP   500             500
3000              3000
VLT TTL1                    Q0          CP      100             100
500               500
HYPERPULL                   Q18         LP      500             500
1000              1000
OPENFLOW                    Q5          CP      300             300
1000              1000
FEFD                        Q6          CP      150             150
1000              1000
TRACEFLOW                   Q16         LP      200             200
500               500
FCoE                        Q12         RP      300             300
2000              2000
L3 LOCAL TERMINATED         Q3          CP      400             400
5000              5000
L3 UNKNOWN/UNRESOLVED ARP   Q7          RP      200             200
3000              3000
L2 DST HIT/BROADCAST        Q1/Q8       CP/RP   200             200
500               500
MULTICAST CATCH ALL         Q7          RP      200             200
500               500
ACL LOGGING                 Q17         LP      200             200
1000              1000
L3 HEADER ERROR/TTL0        Q0          CP      200             200
500               500
IP OPTION/TTL1              Q0          CP      100             100
500               500
VLAN L3 MTU FAIL            Q0          CP      200             200
500               500
```

```
Physical L3 MTU FAIL      Q0           CP      200             200
500             500
SOURCE MISS               Q16          LP      200             200
500             500
STATION MOVE              Q16          LP      200             200
500             500
SFLOW_EGRESS              Q20          LP      5000            5000
3000            3000
SFLOW_INGRESS             Q20          LP      5000            5000
3000            3000
Dell#
```

```
Dell#show protocol-queue-mapping queue-id 3
Protocol               Queue        EgPort   CommitRate(kbps)  Peak Rate(kbps)
CommitBurst(kb) Peak Burst(kb)
--------               -----        ------   ----------------  -------------
--------------  ------------
NTP                    Q3           CP       200               200
2000            2000
FTP                    Q3           CP       400               400
3000            3000
TELNET                 Q3           CP       400               400
2000            2000
SSH                    Q3           CP       400               400
2000            2000
VLT GARP               Q3/Q10       CP/RP    500               500
3000            3000
VLT CTRL - CP CPU      Q3           CP       2000              2000
3000            3000
VLT CTRL - CP & RP CPU Q3/Q10       CP/RP    2000              2000
3000            3000
VLT IPM PDU            Q3/Q10       CP/RP    500               500
3000            3000
L3 LOCAL TERMINATED    Q3           CP       400               400
5000            5000
```

11

Data Center Bridging (DCB)

Data center bridging (DCB) refers to a set of IEEE Ethernet enhancements that provide data centers with a single, robust, converged network to support multiple traffic types, including local area network (LAN), server, and storage traffic.

The Dell Networking operating software commands for data center bridging features include 802.1Qbb priority-based flow control (PFC), 802.1Qaz enhanced transmission selection (ETS), and the data center bridging exchange (DCBX) protocol.

This chapter includes the following sections:

- DCB Command
- PFC Commands
- ETS Commands
- DCBX Commands

Topics:

- DCB Commands
- PFC Commands
- ETS Commands
- DCBX Commands
- dcb-map
- priority-pgid
- priority-group bandwidth pfc
- dcb-map stack-unit all stack-ports all
- dcb pfc-shared-buffer-size
- dcb-buffer-threshold
- priority
- qos-policy-buffer
- dcb-policy buffer-threshold (Interface Configuration)
- show qos dcb-buffer-threshold
- show hardware stack-unit buffer-stats-snapshot
- dcb pfc-total-buffer-size
- show running-config dcb-buffer-threshold
- dcb pfc-queues
- dcb {ets | pfc} enable

DCB Commands

The following DCB command is supported on the Dell Networking OS.

dcb-enable

Enable data center bridging.

C9000 Series

Syntax

`dcb enable[pfc-queues 1|4]`

To disable DCB, use the `no dcb enable` command.

Parameters

pfc-queues	Enter the pfc-queue range. To disable DCB, use the no dcb enable command. The range is from 1 or 2.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

Version

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON .
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, iSCSI is enabled on the unit and the flow control is enabled on all of the interfaces. It is also acts as defaults when the link-level flow control is enabled on one or more interfaces.

To enable DCB, do one of the following:

- Apply the `dcb-input policy` command with the `no pfc-mode` command on to all the interfaces.
- Disable flow-control on all of the interfaces.

Enables priority flow control or enhance transmission selection on interface.

Related Commands

dcb <ets | pfc> enable — enable priority flow control or enhanced transmission selection on interface.

PFC Commands

The following PFC commands are supported on the Dell Networking OS.

clear hardware pfc-nodrop-priority

Clear the drop statistics.

Syntax

```
clear hardware pfc-nodrop-priority l2-dlf drops stack-unit stack-unit-number
port-set port-pipe
```

Parameters

stack-unit *stack-unit-number*	Enter the keywords `stack-unit` and the stack unit number. The range is from 0 to 5.
port-set *port-pipe*	Enter the keywords `port-set` and port-pipe number. The port-pipe number is 0.

Command Modes

EXEC

EXEC Privilege

Command History

Version	Description
9.10(0.0)	Introduced on the C9010, S6000, S6000–ON, Z9100–ON and S6100–ON.

Related Commands

pfc-nodrop-priority l2-dlf drop — configures to drop the unknown unicast packets flooding on lossless priorities.

show hardware pfc-nodrop-priority — displays the packets drop count corresponding to the priority.

clear pfc counters

Clear the PFC TLV counters and PFC statistics on an interface or stack unit.

C9000 Series

Syntax

```
clear pfc counters [port-type slot/port | stack-unit {unit number | all } all
stack-ports all}] | interface {statistics}]
```

Parameters

port-type	Enter the keywords `port-type` then the slot/port information.
stack-unit *unit number*	Enter the keywords `stack-unit` then the stack-unit number to be cleared.
all stack-ports all	Enter the keywords `all stack-ports all` to clear the counters on all interfaces.
statistics	Enter the keyboard `statistics` to clear the hardware PFC counters.

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you do not use the `statistics` parameter, both hardware and DCBx counters clear.

dcb-input

To apply pause or flow control for specified priorities using a configure delay time, create a DCB input policy.

C9000 Series

Syntax

`dcb-input` *`policy-name`*

To delete the DCB input policy, use the `no dcb-input` command.

Parameters

policy-name	Maximum: 32 alphanumeric characters.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Removed from the S-series. Replaced by the dcb-map commands.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Version	Description
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

As soon as you apply a DCB policy with PFC enabled on an interface, DCBx starts exchanging information with PFC-enabled peers. The IEEE802.1Qbb, CEE, and CIN versions of PFC TLV are supported. DCBx also validates PFC configurations received in TLVs from peer devices.

By applying a DCB input policy with PFC enabled, you enable PFC operation on ingress port traffic. To achieve complete lossless handling of traffic, also enable PFC on all DCB egress ports or configure the dot1p priority-queue assignment of PFC priorities to lossless queues (refer to `pfc no-drop queues`).

Related Commands

dcb-map— to configure PFC and ETS on Ethernet ports that support converged Ethernet traffic.

dcb-policy input

Apply the input policy with the PFC configuration to an ingress interface.

C9000 Series

Syntax

`dcb-policy input` *`policy-name`*

To delete the input policy, use the `no dcb-policy input` command.

Parameters

policy-name	Enter the input policy name with the PFC configuration to an ingress interface.

Defaults

none

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Removed from the S-series. Replaced by the dcb-map commands.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

If you apply an input policy with PFC disabled (`no pfc mode on`):

- You can enable link-level flow control on the interface. To delete the input policy, first disable link-level flow control. PFC is then automatically enabled on the interface because an interface is by default PFC-enabled.

- PFC still allows you to configure lossless queues on a port to ensure no-drop handling of lossless traffic.

When you apply an input policy to an interface, an error message is displayed if:

- The PFC dot1p priorities result in more than two lossless port queues globally on the switch.
- You already enabled link-level flow control. PFC and link-level flow control cannot be enabled at the same time on an interface.

In a switch stack, configure all stacked ports with the same PFC configuration.

A DCB input policy for PFC applied to an interface may become invalid if you reconfigure the dot1p-queue mapping. This situation occurs when the new dot1p-queue assignment exceeds the maximum number (2) of lossless queues supported globally on the switch. In this case, all PFC configurations received from PFC-enabled peers are removed and resynchronized with the peer devices.

Traffic may be interrupted when you reconfigure PFC no-drop priorities in an input policy or reapply the policy to an interface.

If the priority group to QoS policy mapping configurations in the DCB output profile are not complete (for example, no priorities are mapped or only some of the priorities are mapped), all eight priorities map to a single priority group with a PGID of 0 for DCBx negotiations.

Related Commands dcb-map— to configure PFC and ETS on Ethernet ports that support converged Ethernet traffic.

dcb-policy input stack-unit stack-ports all

Apply the specified DCB input policy on all ports of the switch stack or a single stacked switch.

C9000 Series

Syntax `dcb-policy input stack-unit {all | stack-unit-id} stack-ports all dcb-input-policy-name`

To remove all DCB input policies applied to the stacked ports and rest the PFC to its default settings, use the `no dcb-policy input stack-unit all` command.

To remove only the DCB input policies applied to the specified switch, use the `no dcb-policy input stack-unit` command.

Parameters

stack-unit-id	Enter the stack unit identification.
dcb-input-policy-name	Enter the policy name for the DCB input policy.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Removed from the S-series. Replaced by the dcb-map commands.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

pfc no-drop queues

Configure the port queues that still function as no-drop queues for lossless traffic.

C9000 Series

Syntax

`pfc no-drop queues` *`queue-range`*

To remove the no-drop port queues, use the `no pfc no-drop queues` command.

Parameters

queue-range	Enter the queue range. Separate the queue values with a comma; specify a priority range with a dash; for example, `pfc no-drop queues 1,3` or `pfc no-drop queues 7` or `pfc no-drop queues 0,7`. The range is from 0 to 3.
queue-range	Enter the queue range. Separate the queue values with a comma; specify a priority range with a dash; for example, `pfc no-drop queues 1,3` or `pfc no-drop queues 2-3`. The range is from 0 to 4.

Defaults No lossless queues are configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

- When you configure lossless queues on an interface, PFC priority configuration is not allowed on the dcb-input profile applied on the interface.
- The maximum number of lossless queues globally supported on the switch is two.

The following lists the dot1p priority-queue assignments

dot1p Value in the Incoming Frame	Description heading
0	0
1	0
2	0
3	1
4	2
5	3
6	3
7	3

pfc-nodrop-priority l2-dlf drop

Configure to drop the unknown unicast packets flooding on lossless priorities.

Syntax

```
pfc-nodrop-priority l2-dlf drop
```

To disable the feature, use the `no pfc-nodrop-priority l2-dlf drop` command.

Parameters

l2-dlf	Enter the keywords `l2-dlf` to drop flooding traffic on lossless priorities.
drop	Enter the keyword `drop` to enable the drop action.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.0)	Introduced on the C9010, S6000, S6000–ON, Z9100–ON and S6100–ON.

Related Commands show hardware pfc-nodrop-priority — displays the packets drop count corresponding to the priority.

pfc priority

Configure the CoS traffic to be stopped for the specified delay.

C9000 Series

Syntax

`pfc priority` *`priority-range`*

To delete the pfc priority configuration, use the `no pfc priority` command.

Parameters

priority-range	Enter the 802.1p values of the frames to be paused. Separate the priority values with a comma; specify a priority range with a dash; for example, pfc priority 1,3,5-7. The range is from 0 to 7.

Defaults

none

Command Modes

DCB INPUT POLICY

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

NOTE: Please note that Dell Networking do not recommend to use this command as it has been deprecated in the current 9.4.(0.0) release. A warning message appears when you try to run this command indicating that you have to use the dcb-map commands in the future.

You can enable any number of 802.1p priorities for PFC. Queues to which PFC priority traffic is mapped are lossless by default. Traffic may be interrupted due to an interface flap (going down and coming up) when you reconfigure the lossless queues for no-drop priorities in a PFC input policy and reapply the policy to an interface.

The maximum number of lossless queues supported on the switch is two.

A PFC peer must support the configured priority traffic (as DCBX detects) to apply PFC.

show dcb

Display the data center bridging status, the number of PFC-enabled ports, and the number of PFC-enabled queues.

C9000 Series

Syntax `show dcb [stack-unit unit-number] [port-set port-set-number]`

Parameters

unit-number	Enter the DCB unit number.
port-set-number	Enter the port-set number.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information Specify a stack-unit number on the Master switch in a stack.

Example

```
Dell# show dcb
stack-unit 1 port-set 0
      DCB Status : Enabled
    PFC Port Count : 56 (current), 56 (configured)
PFC Queue Count : 2 (current), 2 (configured)
```

show hardware pfc-nodrop-priority

View the packets drop count corresponding to the priority.

Syntax `show hardware pfc-nodrop-priority l2-dlf drops stack-unit stack-unit-number port-set port-pipe`

Parameters

stack-unit *stack-unit-number*	Enter the keywords `stack-unit` and the stack unit number. The range is from 0 to 5.
port-set *port-pipe*	Enter the keywords `port-set` and port-pipe number. The port-pipe number is 0.

Command Modes EXEC

EXEC Privilege

Command History

Version	Description
9.10(0.0)	Introduced on the C9010, S6000, S6000–ON, Z9100–ON and S6100–ON.

Example

```
Dell#show hardware pfc-nodrop-priority l2-dlf drops stack-unit 0 port-set 0
-------------------------------------------------
        Priority                          DropCount
-------------------------------------------------
           0                                 0
           1                                 0
           2                                 0
           3                                 0
           4                                 0
           5                                 0
           6                                 0
           7                                 0
```

Related Commands pfc-nodrop-priority l2-dlf drop — configures to drop the unknown unicast packets flooding on lossless priorities.

show interface pfc

Display the PFC configuration applied to ingress traffic on an interface, including priorities and link delay.

C9000 Series

Syntax `show interface port-type slot/port pfc {summary | detail}`

Parameters

port-type slot/ port pfc	Enter the port-type slot and port PFC information.
{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON..
9.2.(0.0)	Down status messages added.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To clear the PFC TLV counters, use the `clear pfc counters interface` *port-type slot/port* command.

To view the PFC show output for multiple ports of a specified slot, you can specify any random port number or a range of ports, or a combination of both.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces tengigabitethernet 10/0-1 pfc summary`. To enter any random number of ports, you can enter a comma-separated string of port numbers, for example `show interfaces tengigabitethernet 10/2,4 pfc summary`

The following describes the `show interface pfc summary` command shown in the following example.

Field	Description
Interface	Interface type with stack-unit and port number.
Admin mode is on Admin is enabled	PFC admin mode is on or off with a list of the configured PFC priorities. When the PFC admin mode is on, PFC advertisements are enabled to be sent and received from peers; received PFC configuration take effect. The admin operational status for a DCBX exchange of PFC configuration is enabled or disabled.
Remote is enabled, Priority list Remote Willing Status is enabled	Operational status (enabled or disabled) of peer device for DCBX exchange of PFC configuration with a list of the configured PFC priorities. Willing status of peer device for DCBX exchange (Willing bit received in PFC TLV): enabled or disable.
Local is enabled	DCBX operational status (enabled or disabled) with a list of the configured PFC priorities.
Operational status (local port)	Port state for current operational PFC configuration: • `Init`: Local PFC configuration parameters were exchanged with the peer. • `Recommend`: Remote PFC configuration parameters were received from the peer. • `Internally propagated`: PFC configuration parameters were received from the configuration source.
PFC DCBX Oper status	Operational status for the exchange of the PFC configuration on the local port: match (up) or mismatch (down).
State Machine Type	Type of state machine used for DCBX exchanges of the PFC parameters: Feature — for legacy DCBX versions; Symmetric — for an IEEE version.
TLV Tx Status	Status of the PFC TLV advertisements: enabled or disabled.
PFC Link Delay	Link delay (in quanta) used to pause specified priority traffic.
Application Priority TLV: FCOE TLV Tx Status	Status of FCoE advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
Application Priority TLV: SCSI TLV Tx Status	Status of ISCSI advertisements in application priority TLVs from the local DCBX port: enabled or disabled.
Application Priority TLV: Local FCOE Priority Map	Priority bitmap the local DCBX port uses in FCoE advertisements in application priority TLVs.

Field	Description
Application Priority TLV: Local ISCSI Priority Map	Priority bitmap the local DCBX port uses in ISCSI advertisements in application priority TLVs.
Application Priority TLV: Remote FCOE Priority Map	Status of FCoE advertisements in application priority TLVs from the remote peer port: enabled or disabled.
Application Priority TLV: Remote ISCSI Priority Map	Status of iSCSI advertisements in application priority TLVs from the remote peer port: enabled or disabled.
PFC TLV Statistics: Input TLV pkts	Number of PFC TLVs received.
PFC TLV Statistics: Output TLV pkts	Number of PFC TLVs transmitted.
PFC TLV Statistics: Error pkts	Number of PFC error packets received.
PFC TLV Statistics: Pause Tx pkts	Number of PFC pause frames transmitted.
PFC TLV Statistics: Pause Rx pkts	Number of PFC pause frames received.

Example (Summary)

```
Dell# show interfaces tengigabitethernet 0/49 pfc summary
Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled, Priority list is 4
  Remote Willing Status is enabled
  Local is enabled
  Oper status is Recommended
  PFC DCBX Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quantams
  Application Priority TLV Parameters :
  ------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8

Dell# show interfaces tengigabitethernet 0/49 pfc detail
  Interface TenGigabitEthernet 0/49
  Admin mode is on
  Admin is enabled
  Remote is enabled
  Remote Willing Status is enabled
  Local is enabled
  Oper status is recommended
  PFC DCBX Oper status is Up
  State Machine Type is Feature
  TLV Tx Status is enabled
  PFC Link Delay 45556 pause quanta
  Application Priority TLV Parameters :
  ------------------------------------
  FCOE TLV Tx Status is disabled
  ISCSI TLV Tx Status is disabled
```

```
  Local FCOE PriorityMap is 0x8
  Local ISCSI PriorityMap is 0x10
  Remote FCOE PriorityMap is 0x8
  Remote ISCSI PriorityMap is 0x8
  0 Input TLV pkts, 1 Output TLV pkts, 0 Error pkts,
  0 Pause Tx pkts, 0 Pause Rx pkts
```

Example (interface port range)

```
Dell#show interfaces tengigabitethernet 10/0-1 pfc summary

Interface TenGigabitEthernet 10/0
     Admin mode is on
     Admin is enabled
     Remote is disabled
     Local is enabled
     Oper status is init
     PFC DCBX Oper status is Down
     Reason: Port Shutdown
     State Machine Type is Symmetric
     TLV Tx Status is enabled
     PFC Link Delay 65535 pause quantams
     Application Priority TLV  Parameters :
     -------------------------------------
     FCOE TLV Tx Status is disabled
     ISCSI TLV Tx Status is disabled
     Local FCOE PriorityMap is 0x0
     Local ISCSI PriorityMap is 0x0


Interface TenGigabitEthernet 10/1
     Admin mode is on
     Admin is enabled
     Remote is disabled
     Local is enabled
     Oper status is init
     PFC DCBX Oper status is Down
     Reason: Port Shutdown
     State Machine Type is Symmetric
     TLV Tx Status is enabled
     PFC Link Delay 65535 pause quantams
     Application Priority TLV  Parameters :
     -------------------------------------
     FCOE TLV Tx Status is disabled
     ISCSI TLV Tx Status is disabled
     Local FCOE PriorityMap is 0x0
     Local ISCSI PriorityMap is 0x0
```

show interface pfc statistics

Display counters for the PFC frames received and transmitted (by dot1p priority class) on an interface.

C9000 Series

Syntax `show interface port-type slot/port pfc statistics`

Parameters

port-type	Enter the port type.
slot/port	Enter the slot/port number. Enter the subport number if a 40G port is fanned-out into 10G ports.

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To view the show output for multiple ports of a specified slot at a time, you can specify any random port number or a range of ports, or a combination of both.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces tengigabitethernet 10/0-4,7 pfc statistics`. To enter any random number of ports, you can enter a comma-separated string of port numbers, for example `show interfaces tengigabitethernet 10/0,9 pfc statistics`

Example (Summary)

```
Dell (conf-if-te-0/1)#show int te 0/1 pfc statistics
Interface TenGigabitEthernet 0/1
Priority    Rx XOFF Frames      Rx Total Frames   Tx Total Frames
-------------------------------------------------------------------

0           0                   0                 0
1           0                   0                 0
2           0                   0                 0
3           0                   0                 0
4           0                   0                 0
5           0                   0                 0
6           0                   0                 0
7           0                   0                 0
```

Example (port range)

```
Dell#show interfaces tengigabitethernet 10/0-1 pfc statistics

Interface TenGigabitEthernet 10/0

Interface  Priority  Rx XOFF Frames  Rx Total Frames  Tx Total Frames
-------------------------------------------------------------------------
Te 10/0    P0         0               0                 0
Te 10/0    P1         0               0                 0
Te 10/0    P2         0               0                 0
Te 10/0    P3         0               0                 0
Te 10/0    P4         0               0                 0
Te 10/0    P5         0               0                 0
Te 10/0    P6         0               0                 0
Te 10/0    P7         0               0                 0

Interface TenGigabitEthernet 10/1

Interface  Priority  Rx XOFF Frames  Rx Total Frames  Tx Total Frames
-------------------------------------------------------------------------
Te 10/1    P0        0               0                0
Te 10/1    P1        0               0                0
```

```
Te 10/1     P2          0                   0                   0
Te 10/1     P3          0                   0                   0
Te 10/1     P4          0                   0                   0
Te 10/1     P5          0                   0                   0
Te 10/1     P6          0                   0                   0
Te 10/1     P7          0                   0                   0
```

ETS Commands

The following ETS commands are supported on the Dell Networking OS.

dcb-enable

Enable data center bridging.

C9000 Series

Syntax

`dcb enable[pfc-queues 1|4]`

To disable DCB, use the `no dcb enable` command.

Parameters

pfc-queues	Enter the pfc-queue range. To disable DCB, use the no dcb enable command. The range is from 1 or 2.

Defaults

None

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

Version

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON .
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

By default, iSCSI is enabled on the unit and the flow control is enabled on all of the interfaces. It is also acts as defaults when the link-level flow control is enabled on one or more interfaces.

To enable DCB, do one of the following:

- Apply the `dcb-input policy` command with the `no pfc-mode` command on to all the interfaces.
- Disable flow-control on all of the interfaces.

Enables priority flow control or enhance transmission selection on interface.

Related Commands dcb <ets | pfc> enable — enable priority flow control or enhanced transmission selection on interface.

dcb-output

To associate an ETS configuration with priority traffic, create a DCB output policy.

C9000 Series

Syntax `dcb-output` *`policy-name`*

To remove the ETS output policy globally, use the `no dcb output` *`policy-name`* command.

Parameters

policy-name	Enter the DCB output policy name. The maximum is 32 alphanumeric characters.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Removed from the S-series. Replaced by the dcb-map commands.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information To associate a priority group with an ETS output policy with scheduling and bandwidth configuration, create a DCB output policy. You can apply a DCB output policy on multiple egress ports. When you apply an ETS output policy on an interface, ETS-configured scheduling and bandwidth allocation take precedence over any configured settings in QoS output policies.

The ETS configuration associated with 802.1 priority traffic in a DCB output policy is used in DCBX negotiation with ETS peers.

Related Commands dcb-map — to configure PFC and ETS on Ethernet ports that support converged Ethernet traffic.

dcb-policy output

Apply the output policy with the ETS configuration to an egress interface.

C9000 Series

Syntax `dcb-policy output policy-name`

To delete the output policy, use the `no dcb-policy output` command.

Parameters

policy-name	Enter the output policy name.

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Removed from the S-series. Replaced by the dcb-map commands.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information When you apply an ETS output policy to on interface, ETS-configured scheduling and bandwidth allocation take precedence over any configured settings in QoS output policies.

When you disable DCB, ETS is disabled by default. When you enable DCB, ETS is enabled for all interfaces that have the default ETS configuration applied (all dot1p priorities in the same group with equal bandwidth allocation).

Related Commands dcb-map— to configure PFC and ETS on Ethernet ports that support converged Ethernet traffic.

clear ets counters

Clear all ETS TLV counters on an interface.

C9000 Series

Syntax `clear ets counters port-type slot/port`

Parameters

port-type	Enter the keywords `port-type` then the slot/port information.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

show interfaces ets

Displays the ETS configuration applied to egress traffic on an interface, including priority groups with priorities and bandwidth allocation.

C9000 Series

Syntax `show interface` *`port-type slot/port`* `ets {summary | detail}`

Parameters

port-type slot/port **ets**	Enter the port-type slot and port ETS information.
{summary | detail}	Enter the keyword `summary` for a summary list of results or enter the keyword `detail` for a full list of results.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
9.2(0.2)	Down status messages added.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To clear ETS TLV counters, use the `clear ets counters interface` *port-type slot/port* command.

To view the ETS show output for multiple ports of a specified slot, you can specify any random port number or a range of ports, or a combination of both.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces tengigabitethernet 10/0-1 ets summary`. To enter any random number of ports, you can enter a comma-separated string of port numbers, for example `show interfaces tengigabitethernet 10/2,4 ets summary`

The following describes the `show interface summary` command shown in the following example.

Field	Description
Interface	Interface type with stack-unit and port number.
Max Supported TC Group	Maximum number of priority groups supported.
Number of Traffic Classes	Number of 802.1p priorities currently configured.
Admin mode	ETS mode: on or off. When on, the scheduling and bandwidth allocation configured in an ETS output policy or received in a DCBX TLV from a peer can take effect on an interface.
Admin Parameters	ETS configuration on local port, including priority groups, assigned dot1p priorities, and bandwidth allocation.
Remote Parameters	ETS configuration on remote peer port, including admin mode (enabled if a valid TLV was received or disabled), priority groups, assigned dot1p priorities, and bandwidth allocation. If ETS admin mode is enabled on the remote port for DCBX exchange, the Willing bit received in ETS TLVs from the remote peer is included.
Local Parameters	ETS configuration on local port, including admin mode (enabled when a valid TLV is received from a peer), priority groups, assigned dot1p priorities, and bandwidth allocation.
Operational status (local port)	Port state for current operational ETS configuration: • `Init`: Local ETS configuration parameters were exchanged with the peer. • `Recommend`: Remote ETS configuration parameters were received from the peer. • `Internally propagated`: ETS configuration parameters were received from the configuration source.
ETS DCBX Oper status	Operational status of the ETS configuration on the local port: match or mismatch.
State Machine Type	Type of state machine used for DCBX exchanges of ETS parameters: Feature — for legacy DCBX versions; Asymmetric — for an IEEE version.
Conf TLV Tx Status	Status of ETS Configuration TLV advertisements: enabled or disabled.
ETS TLV Statistic: Input Conf TLV pkts	Number of ETS Configuration TLVs received.

Field	Description
ETS TLV Statistic: Output Conf TLV pkts	Number of ETS Configuration TLVs transmitted.
ETS TLV Statistic: Error Conf TLV pkts	Number of ETS Error Configuration TLVs received.

Example (Summary)

```
Dell(conf-qos-policy-out-ets)#show interface te 0/3 ets de

Interface TenGigabitEthernet 0/3
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on

Admin Parameters :
------------------
Admin is enabled

TC-grp Priority#   Bandwidth  TSA
-----------------------------------------------
0                  -          -
1      0,1,2       100%       ETS
2      3           0 %        SP
3      4,5,6,7     0 %        SP
4                  -          -
5                  -          -
6                  -          -
7                  -          -

Remote Parameters :
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled

TC-grp Priority#   Bandwidth TSA
-----------------------------------------------
0                  -         -
1      0,1,2       100%      ETS
2      3           0 %       SP
3      4,5,6,7     0 %       SP
4                  -         -
5                  -         -
6                  -         -
7                  -         -

Oper status is init
ETS DCBX Oper status is Down
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled

0 Input Conf TLV Pkts, 1955 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
0 Input Reco TLV Pkts, 1955 Output Reco TLV Pkts, 0 Error Reco TLV Pkts

Dell(conf-qos-policy-out-ets)#do sho int te 0/3 ets de

Interface TenGigabitEthernet 0/3
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on

Admin Parameters :
```

```
------------------
Admin is enabled

TC-grp Priority#   Bandwidth TSA
-----------------------------------------------
0                  -         -
1      0,1,2       100%      ETS
2      3           0 %       SP
3      4,5,6,7     0 %       SP
4                  -         -
5                  -         -
6                  -         -
7                  -         -

Remote Parameters :
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled

TC-grp Priority#   Bandwidth TSA
-----------------------------------------------
0                  -         -
1      0,1,2       100%      ETS
2      3           0 %       SP
3      4,5,6,7     0 %       SP
4                  -         -
5                  -         -
6                  -         -
7                  -         -

Oper status is init
ETS DCBX Oper status is Down
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled

0 Input Conf TLV Pkts, 1955 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
0 Input Reco TLV Pkts, 1955 Output Reco TLV Pkts, 0 Error Reco TLV Pkts

Dell(conf)# show interfaces tengigabitethernet 0/0 ets detail
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters :
------------------
Admin is enabled
TC-grp Priority# Bandwidth TSA
0 0,1,2,3,4,5,6,7 100% ETS
1 0% ETS
2 0% ETS
3 0% ETS
4 0% ETS
5 0% ETS
6 0% ETS
7 0% ETS
Priority# Bandwidth TSA
0 13% ETS
1 13% ETS
2 13% ETS
3 13% ETS
4 12% ETS
5 12% ETS
6 12% ETS
7 12% ETS
Remote Parameters:
```

```
------------------
Remote is disabled
Local Parameters :
------------------
Local is enabled
TC-grp Priority# Bandwidth TSA
0 0,1,2,3,4,5,6,7 100% ETS
1 0% ETS
2 0% ETS
3 0% ETS
4 0% ETS
5 0% ETS
6 0% ETS
7 0% ETS
Priority# Bandwidth TSA
0 13% ETS
1 13% ETS
2 13% ETS
3 13% ETS
4 12% ETS
5 12% ETS
6 12% ETS
7 12% ETS
Oper status is init
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
0 Input Conf TLV Pkts, 0 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
0T LIVnput Traffic Class TLV Pkts, 0 Output Traffic Class TLV Pkts, 0 Error
Traffic
Class
Pkts
```

Example (Detail)

```
Dell(conf)# show interfaces tengigabitethernet 0/0 ets detail
Interface TenGigabitEthernet 0/0
Max Supported TC Groups is 4
Number of Traffic Classes is 8
Admin mode is on
Admin Parameters :
------------------
Admin is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
1                       0%        ETS
2                       0%        ETS
3                       0%        ETS
4                       0%        ETS
5                       0%        ETS
6                       0%        ETS
7                       0%        ETS

Priority#               Bandwidth TSA
0                       13%       ETS
1                       13%       ETS
2                       13%       ETS
3                       13%       ETS
4                       12%       ETS
5                       12%       ETS
6                       12%       ETS
7                       12%       ETS
Remote Parameters:
------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled
TC-grp Priority#        Bandwidth TSA
0      0,1,2,3,4,5,6,7  100%      ETS
```

```
1                         0%        ETS
2                         0%        ETS
3                         0%        ETS
4                         0%        ETS
5                         0%        ETS
6                         0%        ETS
7                         0%        ETS

Priority#                 Bandwidth TSA
0                         13%       ETS
1                         13%       ETS
2                         13%       ETS
3                         13%       ETS
4                         12%       ETS
5                         12%       ETS
6                         12%       ETS
7                         12%       ETS
Oper status is init
Conf TLV Tx Status is disabled
Traffic Class TLV Tx Status is disabled
0 Input Conf TLV Pkts, 0 Output Conf TLV Pkts, 0 Error Conf TLV Pkts
0 Input Traffic Class TLV Pkts, 0 Output Traffic Class TLV Pkts, 0 Error
Traffic Class
TLV
Pkts
```

Example (interface port-range)

```
show interfaces tengigabitethernet 10/0-1 ets summary

Interface TenGigabitEthernet 10/0
Max Supported TC is 3
Number of Traffic Classes is 8
Admin mode is on

Admin Parameters :
------------------
Admin is enabled

PG-grp  Priority#    BW-%     BW-COMMITTED       BW-PEAK     TSA
                      %     Rate(Mbps) Burst(KB) Rate(Mbps) Burst(KB)
-------------------------------------------------------------------------
0      0,1,2,3,4,5,6,7 100 -     -       -       -              ETS
1                          -     -       -       -        -      -
2                          -     -       -       -     -         -
3                          -     -       -       -     -         -
4                          -     -       -       -     -         -
5                          -     -       -       -     -         -
6                          -     -       -       -     -         -
7                          -     -       -       -      -        -

Remote Parameters :
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled

PG-grp  Priority#        BW-%   BW-COMMITTED        BW-PEAK         TSA
                           %   Rate(Mbps) Burst(KB) Rate(Mbps) Burst(KB)
-------------------------------------------------------------------------
0       0,1,2,3,4,5,6,7   100   -        -       -        -      ETS
1                          -     -        -       -        -      -
2                          -     -        -       -        -      -
3                          -     -        -       -        -      -
4                          -     -        -       -        -      -
5                          -     -        -       -        -      -
6                          -     -        -       -        -      -
7                          -     -        -       -        -      -
```

```
Oper status is init
ETS DCBX Oper status is Down
Reason: Port Shutdown
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled



Interface TenGigabitEthernet 10/1
Max Supported TC is 3
Number of Traffic Classes is 8
Admin mode is on

Admin Parameters :
------------------
Admin is enabled

PG-grp  Priority#      BW-%      BW-COMMITTED        BW-PEAK        TSA
                         %     Rate(Mbps) Burst(KB) Rate(Mbps) Burst(KB)
-------------------------------------------------------------------------
0       0,1,2,3,4,5,6,7   100   -        -       -        -       ETS
1                         -     -        -       -        -       -
2                         -     -        -       -        -       -
3                         -     -        -       -        -       -
4                         -     -        -       -        -       -
5                         -     -        -       -        -       -
6                         -     -        -       -        -       -
7                         -     -        -       -        -       -

Remote Parameters :
-------------------
Remote is disabled

Local Parameters :
------------------
Local is enabled

PG-grp  Priority#      BW-%      BW-COMMITTED      BW-PEAK      TSA
                         %    Rate(Mbps) Burst(KB) Rate(Mbps) Burst(KB)
-------------------------------------------------------------------------
0       0,1,2,3,4,5,6,7   100   -     -         -         -      ETS
1                         -     -     -         -         -      -
2                         -     -     -         -         -      -
3                         -     -     -         -         -      -
4                         -     -     -         -         -      -
5                         -     -     -         -         -      -
6                         -     -     -         -         -      -
7                         -     -     -         -         -      -

Oper status is init
ETS DCBX Oper status is Down
Reason: Port Shutdown
State Machine Type is Asymmetric
Conf TLV Tx Status is enabled
Reco TLV Tx Status is enabled
```

DCBX Commands

The following DCBX commands are supported on the Dell Networking OS.

advertise dcbx-tlv

On a DCBX port with a manual role, configure the PFC and ETS TLVs advertised to DCBX peers.

C9000 Series

Syntax

```
advertise dcbx-tlv {ets-conf | ets-reco | pfc} [ets-conf | ets-reco | pfc]
[ets-conf | ets-reco | pfc]
```

To remove the advertised ETS TLVs, use the `no advertise dcbx-tlv` command.

Parameters

{ets-conf | ets-reco | pfc} Enter the PFC and ETS TLVs advertised, where:

- `ets-conf`: enables the advertisement of ETS configuration TLVs.
- `ets-reco`: enables the advertisement of ETS recommend TLVs.
- `pfc`: enables the advertisement of PFC TLVs.

Defaults

All PFC and ETS TLVs are advertised.

Command Modes

PROTOCOL LLDP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

You can configure the transmission of more than one TLV type at a time; for example: `advertise dcbx-tlv ets-conf ets-reco`.

You can enable ETS recommend TLVs (`ets-reco`) only if you enable ETS configuration TLVs (`ets-conf`). To disable TLV transmission, use the `no` form of the command; for example, `no advertise dcbx-tlv pfc ets-reco`.

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

NOTE: The `advertise dcbx-tlv` command is not supported on cascade interfaces or extended ports.

dcbx port-role

Configure the DCBX port role the interface uses to exchange DCB information.

C9000 Series

Syntax

`dcbx port-role {config-source | auto-downstream | auto-upstream | manual}`

To remove DCBX port role, use the `no dcbx port-role {config-source | auto-downstream | auto-upstream | manual}` command.

Parameters

config-source | auto-downstream | auto-upstream | manual

Enter the DCBX port role, where:

- `config-source`: configures the port to serve as the configuration source on the switch.
- `auto-upstream`: configures the port to receive a peer configuration. The configuration source is elected from auto-upstream ports.
- `auto-downstream`: configures the port to accept the internally propagated DCB configuration from a configuration source.
- `manual`: configures the port to operate only on administer-configured DCB parameters. The port does not accept a DCB configuration received form a peer or a local configuration source.

Defaults

Manual

Command Modes

INTERFACE PROTOCOL LLDP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9000 Series.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

NOTE: The `dcbx port-role` command is not supported on cascade interfaces or extended ports.

dcbx version

Configure the DCBX version used on the interface.

C9000 Series

Syntax

`dcbx version {auto | cee | cin | ieee-v2.5}`

To remove the DCBX version, use the `no dcbx version` command.

Parameters

auto | cee | cin | ieee-v2.5

Enter the DCBX version type used on the interface, where:

- `auto`: configures the port to operate using the DCBX version received from a peer.
- `cee`: configures the port to use CDD (Intel 1.01).
- `cin`: configures the port to use Cisco-Intel-Nuova (DCBX 1.0).
- `ieee-v2`: configures the port to use IEEE 802.1az (Draft 2.5).

Defaults

Auto

Command Modes

INTERFACE PROTOCOL LLDP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9 (0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

DCBX requires that you enable LLDP to advertise DCBX TLVs to peers.

Configure DCBX operation at the INTERFACE level on a switch or globally on the switch. To verify the DCBX configuration on a port, use the `show interface dcbx detail` command.

NOTE: The `dcbx version` command is not supported on cascade interfaces or extended ports.

debug dcbx

Enable DCBX debugging.

Syntax

```
debug dcbx {all | auto-detect-timer | config-exchng | fail | mgmt | resource | sem | tlv}
```

To disable DCBX debugging, use the `no debug dcbx` command.

Parameters

{all | auto-detect-timer | config-exchng | fail | mgmt | resource | sem | tlv}

Enter the type of debugging, where:

- `all`: enables all DCBX debugging operations.
- `auto-detect-timer`: enables traces for DCBX auto-detect timers.
- `config-exchng`: enables traces for DCBX configuration exchanges.
- `fail`: enables traces for DCBX failures.
- `mgmt`: enables traces for DCBX management frames.
- `resource`: enables traces for DCBX system resource frames.
- `sem`: enables traces for the DCBX state machine.
- `tlv`: enables traces for DCBX TLVs.

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 .
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

fcoe priority-bits

Configure the FCoE priority advertised for the FCoE protocol in application priority TLVs.

C9000 Series

Syntax

```
fcoe priority-bits priority-bitmap
```

To remove the configured FCoE priority, use the `no fcoe priority-bits` command.

Parameters

priority-bitmap Enter the priority-bitmap range. The range is from 1 to FF.

Defaults 0x8

Command Modes PROTOCOL LLDP

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command is available at the global level only.

iscsi priority-bits

Configure the iSCSI priority advertised for the iSCSI protocol in application priority TLVs.

C9000 Series

Syntax `iscsi priority-bits` *priority-bitmap*

To remove the configured iSCSI priority, use the `no iscsi priority-bits` command.

Parameters

priority-bitmap Enter the priority-bitmap range. The range is from 1 to FF.

Defaults 0x10

Command Modes PROTOCOL LLDP

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Inroduced on the C9010.

Version	Description
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information This command is available at the global level only.

show interface dcbx detail

Display the DCBX configuration on an interface.

C9000 Series

Syntax `show interface port-type slot/port dcbx detail`

Parameters

port-type	Enter the port type.
slot/port	Enter the slot/port number.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
9.2.(0.0)	Down status messages added.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information To clear DCBX frame counters, use the `clear dcbx counters interface stack-unit/port` command.

To view the DCBX show output for multiple ports of a specified slot, you can specify any random number of ports separated by commas or a hyphenated range of ports.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces tengigabitethernet 10/0-1 dcbx detail`. To enter any random number of ports, you can enter a comma-separated string of port numbers, for example `show interfaces tengigabitethernet 10/2,4 dcbx detail`

NOTE: The multiple port range value is supported only for the Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, Fast Ethernet, FC, Port Channel, and VLAN interfaces.

The following describes the `show interface dcbx detail` command shown in the following example.

Field	Description
Interface	Interface type with chassis slot and port number.
Port-Role	Configured the DCBX port role: auto-upstream, auto-downstream, config-source, or manual.
DCBX Operational Status	Operational status (enabled or disabled) used to elect a configuration source and internally propagate a DCB configuration. The DCBX operational status is the combination of PFC and ETS operational status.
Configuration Source	Specifies whether the port serves as the DCBX configuration source on the switch: true (yes) or false (no).
Local DCBX Compatibility mode	DCBX version accepted in a DCB configuration as compatible. In auto-upstream mode, a port can only receive a DCBX version supported on the remote peer.
Local DCBX Configured mode	DCBX version configured on the port: CEE, CIN, IEEE v2.5, or Auto (port auto-configures to use the DCBX version received from a peer).
Peer Operating version	DCBX version that the peer uses to exchange DCB parameters.
Local DCBX TLVs Transmitted	Transmission status (enabled or disabled) of advertised DCB TLVs (see TLV code at the top of the show command output).
Local DCBX Status: DCBX Operational Version	DCBX version advertised in Control TLVs.
Local DCBX Status: DCBX Max Version Supported	Highest DCBX version supported in Control TLVs.
Local DCBX Status: Sequence Number	Sequence number transmitted in Control TLVs.
Local DCBX Status: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs.
Local DCBX Status: Protocol State	Current operational state of the DCBX protocol: ACK or IN-SYNC.
Peer DCBX Status: DCBX Operational Version	DCBX version advertised in Control TLVs received from the peer device.
Peer DCBX Status: DCBX Max Version Supported	Highest DCBX version supported in Control TLVs received from the peer device.

Field	Description
Peer DCBX Status: Sequence Number	Sequence number transmitted in Control TLVs received from the peer device.
Peer DCBX Status: Acknowledgment Number	Acknowledgement number transmitted in Control TLVs received from the peer device.
Total DCBX Frames transmitted	Number of DCBX frames sent from the local port.
Total DCBX Frames received	Number of DCBX frames received from the remote peer port.
Total DCBX Frame errors	Number of DCBX frames with errors received.
Total DCBX Frames unrecognized	Number of unrecognizable DCBX frames received.

Example

```
Dell#show interfaces te 10/3 dcbx detail

E-ETS Configuration TLV enabled          e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled         r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled          p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled  f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled i-Application Priority for iSCSI disabled
---------------------------------------------------------------------------------

Interface TenGigabitEthernet 10/3
   Port Role is Auto-Upstream
   DCBX Operational Status is Disabled
   Reason: Port Shutdown
   Is Configuration Source? FALSE
   Local DCBX Compatibility mode is AUTO
   Local DCBX Configured mode is AUTO
   Peer Operating version is Not Detected
   Local DCBX TLVs Transmitted: ErPfi
     Total DCBX Frames transmitted 8
     Total DCBX Frames received 3
     Total DCBX Frame errors 0
     Total DCBX Frames unrecognized 0
```

Example- port range

```
Dell#show interfaces tengigabitethernet 10/0-1 dcbx detail

E-ETS Configuration TLV enabled          e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled         r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled          p-PFC Configuration TLV disabled
F-Application priority for FCOE enabled  f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled i-Application Priority for iSCSI disabled
---------------------------------------------------------------------------------

Interface TenGigabitEthernet 10/0
   Port Role is Manual
   DCBX Operational Status is Disabled
   Reason: Port Shutdown
   Is Configuration Source? FALSE
   Local DCBX Compatibility mode is AUTO
   Local DCBX Configured mode is AUTO
   Peer Operating version is Not Detected
   Local DCBX TLVs Transmitted: ERPfi
     Total DCBX Frames transmitted 0
     Total DCBX Frames received 0
     Total DCBX Frame errors 0
     Total DCBX Frames unrecognized 0

E-ETS Configuration TLV enabled           e-ETS Configuration TLV disabled
R-ETS Recommendation TLV enabled          r-ETS Recommendation TLV disabled
P-PFC Configuration TLV enabled           p-PFC Configuration TLV disabled
```

```
F-Application priority for FCOE enabled   f-Application Priority for FCOE disabled
I-Application priority for iSCSI enabled  i-Application Priority for iSCSI disabled
------------------------------------------------------------------------------

Interface TenGigabitEthernet 10/1
   Port Role is Manual
   DCBX Operational Status is Disabled
   Reason: Port Shutdown
   Is Configuration Source? FALSE
   Local DCBX Compatibility mode is AUTO
   Local DCBX Configured mode is AUTO
   Peer Operating version is Not Detected
   Local DCBX TLVs Transmitted: ERPfi
     Total DCBX Frames transmitted 0
     Total DCBX Frames received 0
     Total DCBX Frame errors 0
     Total DCBX Frames unrecognized 0
```

dcb-map

Create a DCB map to configure priority flow control (PFC) and enhanced transmission selection (ETS) on Ethernet ports that support converged Ethernet traffic. Apply the DCB map to an Ethernet interface.

C9000 Series

Syntax `dcb-map map-name`

Parameters

map-name	Enter a DCB map name. The maximum number of alphanumeric characters is 32.

Defaults None. There are no pre-configured PFC and ETS settings on S5000 Ethernet interfaces.

Command Modes CONFIGURATION

INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810 and S6000 platforms.

Usage Information A DCB map is a template used to configure DCB parameters and apply them on converged Ethernet interfaces. DCB parameters include priority-based flow control (PFC) and enhanced traffic selection (ETS).

To display the PFC and ETS settings in DCB maps, enter the `show qos dcb-map` command.

Use the `dcb-map` command to create a DCB map to specify PFC and ETS settings and apply it on Ethernet ports. After you apply a DCB map to an interface, the PFC and ETS settings in the map are applied when the Ethernet port is enabled. DCBx is enabled on Ethernet ports by default.

The `dcb-map` command is supported only on physical Ethernet interfaces.

To remove a DCB map from an interface, enter the `no dcb-map` *`map-name`* command in Interface configuration mode.

priority-pgid

Assign 802.1p priority traffic to a priority group in a DCB map.

C9000 Series

Syntax

`priority-pgid` *`dot1p0_group-num dot1p1_group-num dot1p2_group-num dot1p3_group-num dot1p4_group-num dot1p5_group-num dot1p6_group-num dot1p7_group-num`*

Parameters

dot1p0–7_group-num	Enter the priority group number for each 802.1p class of traffic in a DCB map.

Defaults

None

Command Modes

DCB MAP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S6000 platforms.

Usage Information

PFC and ETS settings are not pre-configured on Ethernet ports. You must use the `dcb-map` command to configure different groups of 802.1p priorities with PFC and ETS settings.

Using the `priority-pgid` command, you assign each 802.1p priority to one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group. For example, the `priority-pgid 0 0 0 1 2 4 4 4` command creates the following groups of 802.1p priority traffic:

- Priority group 0 contains traffic with dot1p priorities 0, 1, and 2.
- Priority group 1 contains traffic with dot1p priority 3.
- Priority group 2 contains traffic with dot1p priority 4.
- Priority group 4 contains traffic with dot1p priority 5, 6, and 7.

To remove a priority-pgid configuration from a DCB map, enter the `no priority-pgid` command.

priority-group bandwidth pfc

Configure the ETS bandwidth allocation and PFC mode used to manage port traffic in an 802.1p priority group.

C9000 Series

Syntax `priority-group` *`group-num`* `{bandwidth` *`percentage`*`| strict-priority} pfc {on | off}`

Parameters

priority-group *group-num*	Enter the keyword `priority-group` followed by the number of an 802.1p priority group. Use the `priority-pgid` command to create the priority groups in a DCB map.
bandwidth *percentage*	Enter the keyword `bandwidth` followed by a bandwidth percentage allocated to the priority group. The range of valid values is 1 to 100. The sum of all allocated bandwidth percentages in priority groups in a DCB map must be 100%.
strict-priority	Configure the priority-group traffic to be handled with strict priority scheduling. Strict-priority traffic is serviced first, before bandwidth allocated to other priority groups is made available.
pfc {on | off}	Configure whether priority-based flow control is enabled (on) or disabled (off) for port traffic in the priority group.

Defaults None

Command Modes DCB MAP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON..
9.7(0.0)	Introduced on the S6000-ON.
9.6(0.0)	Added support to configure peak and committed rate on the S6000 platform.
9.3(0.0)	Introduced on the S4810, S6000 platforms.

Usage Information

Use the `dcb-map` command to configure priority groups with PFC and/or ETS settings and apply them to Ethernet interfaces.

Use the `priority-pgid` command to map 802.1p priorities to a priority group. You can assign each 802.1p priority to only one priority group. A priority group consists of 802.1p priority values that are grouped together for similar bandwidth allocation and scheduling, and that share latency and loss requirements. All 802.1p priorities mapped to the same queue must be in the same priority group.

Repeat the `priority-group bandwidth pfc` command to configure PFC and ETS traffic handling for each priority group in a DCB map.

You can enable PFC on a maximum of two priority queues.

If you configure more than one priority group as strict priority, the higher numbered priority queue is given preference when scheduling data traffic.

If a priority group does not use its allocated bandwidth, the unused bandwidth is made available to other priority groups.

To remove a priority-group configuration in a DCB map, enter the `no priority-group bandwidth pfc` command.

By default, equal bandwidth is assigned to each dot1p priority in a priority group. Use the `bandwidth` parameter to configure the bandwidth percentage assigned to a priority group. The sum of the bandwidth allocated to all priority groups in a DCB map must be 100% of the bandwidth on the link. You must allocate at least 1% of the total port bandwidth to each priority group.

dcb-map stack-unit all stack-ports all

Apply the specified DCB map on all ports of the switch stack.

C9000 Series

Syntax

`dcb-map stack-unit all stack-ports all` *`dcb-map-name`*

To remove the PFC and ETS settings in a DCB map from all stack units, use the `no dcb-map stack-unit all stack-ports all` command.

Parameters

dcb-map-name	Enter the name of the DCB map.

Defaults

None

Command Modes

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON..
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810 and S6000 platforms.

Usage Information

The `dcb-map stack-unit all stack-ports all` command overwrites any previous DCB maps applied to stack ports.

dcb pfc-shared-buffer-size

Configure the maximum amount of shared buffer size for PFC packets in kilobytes.

You must configure the shared buffer size to be less than the total PFC buffer size. If the buffer size and DCB buffer threshold settings are applied on one or more ports, a validaiton is performed to determine whether following condition is satisfied: Shared-pfc-buffer-size <= (Total-pfc-buffer-size - Σpfc priority <> buffer-size on each port, priority).

If the preceding condition is not satisfied by the shared PFC buffer size value, the configuration is not saved and a system logging message is generated stating that the shared buffer size that you attempt to specify cannot be configured because of the existing total buffer space

on the system being lower than the shared buffer size. You must either enter a smaller value for the shared buffer size or increase the total buffer size appropriately by using the `dcb pfc-total- buffer-size` command.

C9000 Series

Syntax `dcb pfc-shared—buffer—size KB`

Parameters

KB	Enter a number in the range of 0 to 7787.

Default The default is 1 KB for S6000 platforms.

Command Modes CONFIGURATION mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S4820T, and S6000 platforms.

Usage Information Configure the maximum shared buffer available for PFC traffic. You can choose to increase or decrease the shared buffer that is currently allocated in the system by default. You must configure the shared buffer size to be less than the total PFC buffer size. If the buffer size and DCB buffer threshold settings are applied on one or more ports, a validation is performed to determine whether following condition is satisfied: If the preceding condition is not satisfied by the shared PFC buffer size value, the configuration is not saved and a system logging message is generated as follows:

Shared-pfc-buffer-size <= (Total-pfc-buffer-size - Σpfc priority <> buffer-size on each port, priority).

```
     Dell(conf)#dcb pfc-shared-buffer-size  2000
     %ERROR: pfc shared buffer size configured cannot accommodate existing
buffer requirement in the system.
```

Example

```
Dell(conf)#dcb pfc-shared-buffer-size  5000
```

dcb-buffer-threshold

Configure the profile name for the DCB buffer threshold.

C9000 Series

Syntax `dcb buffer—threshold profile-name`

Parameters

profile-name	Enter the name of the profile, which can be a string of up to 32 characters in length.

Default None

Command Modes CONFIGURATION mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S4820T, and S6000 platforms.

Usage Information When you enter the profile name, you enter the DCB buffer threshold configuration mode. You can specify the shared buffer threshold limit, the ingress buffer size, buffer limit for pausing the acceptance of packets, and the buffer offset limit for resuming the acceptance of received packets.

priority

Configure the priority for the PFC threshold to be allocated to the buffer space parameters.

C9000 Series

Syntax `priority` *`value`* `buffer-size` *`size`* `pause-threshold` *`threshold-value`* `resume-offset` *`threshold-value`* `shared-threshold-weight` *`size`*

Parameters

priority	Specify the priority of the queue for which the buffer space settings apply
value	Enter a number in the range of 0 to 7 to denote the priority to be allocated to the dynamic buffer control mechanism
buffer-size	Ingress buffer size
size	Size of the ingress buffer in KB. Enter a number in the range of 0 to 7787. The default is 45 KB.
pause-threshold	Buffer limit for pause frames to be sent
threshold-value	Buffer limit at which the port sends the pause to peer in KB. Enter a number in the range of 0 to 7787. The default is 10 KB.
resume-offset	Buffer offset limit for resuming in KB
threshold-value	Buffer offset limit at which the port resumes the peer in KB. Enter a number in the range of 1 to 7787. The default is 10 KB.
shared-threshold-weight	Buffer shared threshold weight
size	Weightage of the priorities on the shared buffer size in the system. Enter a number in the range of 0 to 9. The default shared threshold weight is 10.

Default The default size of the ingress buffer is 45 KB. The default buffer limit at which the port sends the pause to peer and recommences the sending of packets to the peer is 10 KB. The default threshold weight of the shared buffer space is 10.

Command Modes DCB-BUFFER-THRESHOLD mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S4820T, and S6000 platforms.

Usage Information

For each priority, you can specify the shared buffer threshold limit, the ingress buffer size, buffer limit for pausing the acceptance of packets, and the buffer offset limit for resuming the acceptance of received packets. When PFC detects congestion on a queue for a specified priority, it sends a pause frame for the 802.1p priority traffic to the transmitting device.

You can use the `priority` command to set up both the administrative and peer-related PFC priorities. For example, you can configure the intended buffer configuration for all eight priorities. If you configure the number of lossless queues as 4 and if the administrator-configured priorities configured within the DCB input policy is applied, then the configuration for those priorities are pre-designed. However, if the peer-provided priorities are applied, although a DCB input policy is present, the peer-provided priorities become effective for buffer configuration. This method of configuration provides an easy and flexible technique to accommodate both administratively-configured and peer-configured priorities.

Example

```
Dell(conf-dcb-buffer-thr)#priority 0 buffer-size 52 pause-threshold 16 resume-
offset 10 shared-threshold-weight 7
```

qos-policy-buffer

Create a QoS policy buffer and enter the configuration mode to configure the no-drop queues, ingress buffer size, buffer limit for pausing, and buffer offset limit for resuming. .

C9000 Series

Syntax

```
qos-policy-buffer queue queue-num pause no-drop queue buffer-size size pause-
threshold threshold-value resume-offset threshold-value shared-threshold-weight
size
```

Parameters

policy-name	Name of the QoS policy buffer that is applied to an interface for this setting to be effective in conjunction with the DCB input policy. You can specify the shared buffer threshold limit, the ingress buffer size, buffer limit for pausing the acceptance of packets, and the buffer offset limit for resuming the acceptance of received packets. This method of configuration enables different peer-provided and administrative priorities to be set up because the intended queue is directly configured instead of determining the priority to queue mapping for local and remote parameters.
queue 0 to queue 7	Specify the queue number to which the QoS policy buffer parameters apply
pause	Pause frames to be sent at the specified buffer limit levels and pause packet settings
no-drop	The packets for this queue must not be dropped
value	Enter a number in the range of 0 to 7 to denote the priority to be allocated to the dynamic buffer control mechanism

buffer-size	Ingress buffer size
size	Size of the ingress buffer in KB. Enter a number in the range of 0 to 7787. The default is 45 KB.
pause-threshold	Buffer limit for pause frames to be sent
threshold-value	Buffer limit at which the port sends the pause to peer in KB. Enter a number in the range of 0 to 7787. The default is 10 KB.
resume-offset	Buffer offset limit for resuming in KB
threshold-value	Buffer offset limit at which the port resumes the peer in KB. Enter a number in the range of 1 to 7787. The default is 10 KB.
shared-threshold-weight	Buffer shared threshold weight
size	Weightage of the priorities on the shared buffer size in the system. Enter a number in the range of 0 to 9. The default shared threshold weight is 10.

Default The default size of the ingress buffer is 45 KB. The default buffer limit at which the port sends the pause to peer and recommences the sending of packets to the peer is 10 KB. The default threshold weight of the shared buffer space is 10.

Command Modes DCB-BUFFER-THRESHOLD mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S4820T, S6000, and MXL platforms.

Usage Information You must apply this buffer policy at the interface level for the attributes to be applicable in conjunction with the DCB input policy.

For each QoS policy buffer, you can specify the shared buffer threshold limit, the ingress buffer size, buffer limit for pausing the acceptance of packets, and the buffer offset limit for resuming the acceptance of received packets. When PFC detects congestion on a queue for a specified priority, it sends a pause frame for the 802.1p priority traffic to the transmitting device.

You can use set up both the administrative and peer-related PFC priorities. For example, you can configure the intended buffer configuration for all 8 priorities. If you configure the number of lossless queues as 4 and if the administrator-configured priorities configured within the DCB input policy is applied, then the configuration for those priorities are pre-designed. However, if the peer-provided priorities are applied, although a DCB input policy is present, the peer-provided priorities become effective for buffer configuration. This method of configuration provides an easy and flexible technique to accommodate both administratively-configured and peer-configured priorities.

Example

```
Dell(conf)# qos-policy-buffer test
Dell(conf-qos-policy-buffer)#queue 0  pause no-drop buffer-size 128000 pause-
threshold 103360 resume-threshold 83520
```

```
Dell(conf-qos-policy-buffer)# queue 4  pause no-drop buffer-size 128000 pause-
threshold 103360 resume-threshold 83520
```

dcb-policy buffer-threshold (Interface Configuration)

Assign the DCB policy to the DCB buffer threshold profile on interfaces. This setting takes precedence over the global buffer-threshold setting.

C9000 Series

Syntax `dcb-policy buffer-threshold profile-name`

Parameters

buffer-threshold	Configure the profile name for the DCB buffer threshold
profile-name	Enter the name of the profile, which can be a string of up to 32 characters in length.

Default None

Command Modes INTERFACE mode

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S4820T, and S6000 platforms.

Usage Information You can configure up to a maximum of four lossless (PFC) queues. By configuring four lossless queues, you can configure four different priorities and assign a particular priority to each application that your network is used to process. For example, you can assign a higher priority for time-sensitive applications and a lower priority for other services, such as file transfers. You can configure the amount of buffer space to be allocated for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to effectively manage and administer the behavior of lossless queues.

show qos dcb-buffer-threshold

Display the DCB buffer threshold assigned to a QoS policy.

C9000 Series

Syntax `show qos dcb buffer-threshold {name}`

Parameters

name	Enter the name of the profile, which can be a string of up to 32 characters in length.

Command Modes

EXEC

EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S6000 platform.

Usage Information

The following table describes the output fields displayed for the `show` command:

Field	Description
Name	Name of the DCB buffer threshold profile
Buffer threshold parameters	Buffer size allocated for the PFC priority queue and the priority of the queue

Example

```
Dell#show qos dcb buffer-threshold

Name   :      test1
Buffer threshold parameters:
pfc priority 0 buffer-size 40
pfc priority 3 buffer-size 50
```

show hardware stack-unit buffer-stats-snapshot

View the buffer statistics tracking resource information with polling details and historical snapshots.

Syntax

```
show hardware stack-unit stack-unit-number buffer-stats-snapshot unit number
resource X history Y
```

Parameters

stack-unit *unit-number*	Unique ID of the stack unit to select a particular stack member and then enter one of the following command options to display a collection of data based on the option entered.
buffer-stats-snapshot unit *number*	Display the historical snapshot of buffer statistical values
unit	Enter the keyword `unit` along with a port-pipe number, then the keyword counters to display the counters on the selected port-pipe. The range is 0 to 0.
resource *X*	Buffer and traffic manager resources usage, where X can be one of the following: • All - Ingress and Egress resources snapshots • Port {id |all} queue {all} - egress queue-level snapshot for both unicast and multicast packets • Port {id |all} queue ucast {id | all} - egress queue-level snapshot for unicast packets only • Port {id |all} queue mcast {id | all} - egress queue-level snapshot for multicast packets only • Port {id |all} prio-group {id | all} - ingress priority-group level snapshot

history *Y* Historical snapshot details of buffer space statistics, where *Y* can be one of the following:

- Instance {all | id} - Displays the information for all instances or the specified instance of the snapshot.
- Summary - Displays the consolidated information pertaining to the preceding three instances of the snapshot values collected in history.

Command Modes

EXEC

EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S6000 platform.

Usage Information

When you enter the `instance all` option, `show hardware stack-unit` *`unit-number`* `buffer-stats-snapshot unit 0 resource X` output for all available instances on the history collection is displayed.

When you enter the `instance id` option, `show hardware stack-unit` *`unit-number`* `buffer-stats-snapshot unit 0 resource X` for specified instance alone is displayed.

When you enter the `summary`option, `show hardware stack-unit` *`stack-unit-number`* `buffer-stats-snapshot unit 0 resource X` will be enhanced to display the total buffered cells, shared cells, headroom cells for last 5 instances in the table format.

If information for specified instance id is not available when you enter the show command, which occurs if you issue the command before the time elapsed for the snapshot to be captured for that instance ID, the following informational message is displayed on the console:`%Info: Data for instance id id is not available.`

If information for specified instance id id is not available when you enter the show command, which occurs if you issue the command before the time elapsed for the snapshot to be captured for that instance ID, the following informational message is displayed on the console:`%Info: Data for instance id id is not available.`

For example, if you configured 5 as the maximum instances with linear periodicity and a polling interval of 10 seconds, 1 as the multiplier, then 5 instances will be polled at 10, 20, 30, 40, and 50 seconds incrementally. If you attempt to enter the show command to display the fifth instance after 30 seconds of enabling polling, the aforementioned information message is shown.

If specified instance ID is higher than the size of the maximum number of snapshot instances configured, the following error message is displayed on the console:`%Error: Instance Id is not valid. Configured max snapshot instances are <max-instances>`

If you configured the maximum number of instances as 5 and attempt to view the buffer statistics tracking details for the instance ID of 6, the aforementioned error is shown.

In the following example, the Headroom Cells field indicates the amount of shared buffer area that is allocated to store packets that are received after the pause frame is received or a priority-based flow control pause frame is

enabled. When an inbound interface halts the sending of traffic, it must have the buffer space to save all of the packets currently in the buffer, and also all of the packets that were received before the device stops the sending of packets. Headroom space is used for high-priority traffic that needs to be queued and preserved above the input queue limit, such as keepalives and hello messages.

You can use the sample command output to obtain a consolidated, whole-scale set of statistical counters of buffer resource utilization in the system and identify the ports that you want. All resources will be cleared after their values are displayed.

Example: Headroom Cells

```
Dell#show hardware stack-unit 0 buffer-stats-snapshot unit 0 resource all
Stack-unit: 0 unit: 0 port: 1 (interface Fo 0/0)
---------------------------------------
PG#     SHARED CELLS     HEADROOM CELLS
---------------------------------------
0       0                0
1       0                0
2       0                0
3       0                0
4       0                0
5       0                0
6       0                0
7       0                0

---------------------------------------
Q# TYPE     Q#     TOTAL BUFFERED CELLS
---------------------------------------
UCAST       0      0
UCAST       1      0
UCAST       2      0
UCAST       3      0
UCAST       4      0
UCAST       5      0
UCAST       6      0
UCAST       7      0
UCAST       8      0
UCAST       9      0
UCAST       10     0
UCAST       11     1
MCAST       0      0
MCAST       1      0
MCAST       2      0
MCAST       3      0
MCAST       4      0
MCAST       5      0
MCAST       6      0
MCAST       7      0
MCAST       8      0

Stack-unit: 0 unit: 0 port: 5 (interface Fo 0/4)
---------------------------------------
PG#     SHARED CELLS     HEADROOM CELLS
---------------------------------------
0       0                0
1       0                0
2       0                0
3       0                0
4       0                0
5       0                0
6       0                0
7       0                0

---------------------------------------
Q# TYPE     Q#     TOTAL BUFFERED CELLS
---------------------------------------
UCAST       0      0
```

```
UCAST       1       0
UCAST       2       0
UCAST       3       0
UCAST       4       0
UCAST       5       0
UCAST       6       0
UCAST       7       0
UCAST       8       0
UCAST       9       0
UCAST       10      0
UCAST       11      0
MCAST       0       0
MCAST       1       0
MCAST       2       0
MCAST       3       0
MCAST       4       0
MCAST       5       0
MCAST       6       0
MCAST       7       0
MCAST       8       0
<… snip …>
Stack-unit: 0 unit: 0 port: 104 (interface Te 0/124)
---------------------------------------
PG#     SHARED CELLS     HEADROOM CELLS
---------------------------------------
0       0                0
1       0                0
2       0                0
3       0                0
4       0                0
5       0                0
6       0                0
7       0                0

----------------------------------------
Q# TYPE     Q#     TOTAL BUFFERED CELLS
----------------------------------------
UCAST       0      0
UCAST       1      0
UCAST       2      0
UCAST       3      0
UCAST       4      0
UCAST       5      0
UCAST       6      0
UCAST       7      0
UCAST       8      0
UCAST       9      0
UCAST       10     0
UCAST       11     1
MCAST       0      0
MCAST       1      0
MCAST       2      0
MCAST       3      0
MCAST       4      0
MCAST       5      0
MCAST       6      0
MCAST       7      0
MCAST       8      0
```

Example: Number of instances

If only two instances are available when the show command is issued, only

two instances are displayed in the summary output.

```
-----------------------------------------------------------------
Q# TYPE     Q#                        TOTAL BUFFERED CELLS
                                  Instance 1  Instance 2
                                  10S            20S
-----------------------------------------------------------------
```

```
UCAST        2          5        4               1
UCAST        3          2        0
UCAST        11         0        3
MCAST        4          0        0

Dell#show hardware stack-unit 0 buffer-stats-snapshot unit 0
resource port 5 prio-group all history summary

Stack-unit 0 unit 0 port 5 (interface te 0/4)
--------------------------------------------------------------------------------
PG# Instance 1  Instance 2   Instance 3   Instance 4   Instance 5
   Shared Hdrm  Shared Hdrm  Shared Hdrm Shared Hdrm  Shared Hdrm[in CELLS]
--------------------------------------------------------------------------------
6     9     2     0     0     1     0     4     1     7     1
7     0     0     0     0     1     0     0     0     0     0
```

To determine the port that is congested and monitor all queues

(including multicast and unicast queues] only on that port:

```
Dell#$show hardware stack-unit 0 buffer-stats-snapshot unit 0
resource port 1 queue all
Stack-unit: 0 unit: 0 port: 1 (interface Fo 0/0)
---------------------------------------
Q# TYPE     Q#     TOTAL BUFFERED CELLS
---------------------------------------
UCAST       0      0
UCAST       1      0
UCAST       2      0
UCAST       3      0
UCAST       4      0
UCAST       5      0
UCAST       6      0
UCAST       7      0
UCAST       8      0
UCAST       9      0
UCAST       10     0
UCAST       11     1
MCAST       0      0
MCAST       1      0
MCAST       2      0
MCAST       3      0
MCAST       4      0
MCAST       5      0
MCAST       6      0
MCAST       7      0
MCAST       8      0
Dell#
```

To examine the port that is congested and monitor all multicast queues on that port:

```
Dell#show hardware stack-unit 0 buffer-stats-snapshot unit 0
resource port 1 queue mcast all
Stack-unit: 0 unit: 0 port: 1 (interface Fo 0/0)
---------------------------------------
Q# TYPE     Q#     TOTAL BUFFERED CELLS
---------------------------------------
MCAST       0      0
MCAST       1      0
MCAST       2      0
MCAST       3      0
MCAST       4      0
MCAST       5      0
MCAST       6      0
MCAST       7      0
MCAST       8      0
Dell#
```

To determine the port that is congested and monitor all the unicast Queues on that port:

```
Dell#show hardware stack-unit 0 buffer-stats-snapshot unit 0
resource port 1 queue ucast all
Stack-unit: 0 unit: 0 port: 1 (interface Fo 0/0)
----------------------------------------
Q# TYPE     Q#     TOTAL BUFFERED CELLS
----------------------------------------
UCAST       0      0
UCAST       1      0
UCAST       2      0
UCAST       3      0
UCAST       4      0
UCAST       5      0
UCAST       6      0
UCAST       7      0
UCAST       8      0
UCAST       9      0
UCAST       10     0
UCAST       11     0
Dell#
```

To identify the port that is congested and monitor all the priority groups on that particular port:

```
Dell#show hardware stack-unit 0 buffer-stats-snapshot unit 0
resource port 1 prio all
Stack-unit: 0 unit: 0 port: 1 (interface Fo 0/0)
----------------------------------------
PG#     SHARED CELLS     HEADROOM CELLS
----------------------------------------
0       0                0
1       0                0
2       0                0
3       0                0
4       0                0
5       0                0
6       0                0
7       0                0
Dell#
```

To determine the specific priority group, unicast or multicast queue

that is congested and monitor that queue separately:

```
Dell#show hardware stack-unit 0 buffer-stats-snapshot unit 0
resource port 1 prio 6
Stack-unit: 0 unit: 0 port: 1 (interface Fo 0/0)
----------------------------------------
PG#     SHARED CELLS     HEADROOM CELLS
----------------------------------------
6       0                0
```

Example: Headroom Cells

```
Dell#show hardware stack-unit 0 buffer-stats-snapshot unit 0 resource all
Stack-unit: 0 unit: 0 port: 1 (interface Fo 0/0)
----------------------------------------
PG#     SHARED CELLS     HEADROOM CELLS
----------------------------------------
0       0                0
1       0                0
2       0                0
3       0                0
4       0                0
5       0                0
6       0                0
7       0                0
```

```
----------------------------------------
Q# TYPE     Q#     TOTAL BUFFERED CELLS
----------------------------------------
UCAST       0      0
UCAST       1      0
UCAST       2      0
UCAST       3      0
UCAST       4      0
UCAST       5      0
UCAST       6      0
UCAST       7      0
UCAST       8      0
UCAST       9      0
UCAST       10     0
UCAST       11     1
MCAST       0      0
MCAST       1      0
MCAST       2      0
MCAST       3      0
MCAST       4      0
MCAST       5      0
MCAST       6      0
MCAST       7      0
MCAST       8      0

Stack-unit: 0 unit: 0 port: 5 (interface Fo 0/4)
----------------------------------------
PG#     SHARED CELLS     HEADROOM CELLS
----------------------------------------
0       0                0
1       0                0
2       0                0
3       0                0
4       0                0
5       0                0
6       0                0
7       0                0

----------------------------------------
Q# TYPE     Q#     TOTAL BUFFERED CELLS
----------------------------------------
UCAST       0      0
UCAST       1      0
UCAST       2      0
UCAST       3      0
UCAST       4      0
UCAST       5      0
UCAST       6      0
UCAST       7      0
UCAST       8      0
UCAST       9      0
UCAST       10     0
UCAST       11     0
MCAST       0      0
MCAST       1      0
MCAST       2      0
MCAST       3      0
MCAST       4      0
MCAST       5      0
MCAST       6      0
MCAST       7      0
MCAST       8      0
<… snip …>
Stack-unit: 0 unit: 0 port: 104 (interface Te 0/124)
----------------------------------------
PG#     SHARED CELLS     HEADROOM CELLS
----------------------------------------
0       0                0
```

```
1       0               0
2       0               0
3       0               0
4       0               0
5       0               0
6       0               0
7       0               0
---------------------------------------
Q# TYPE     Q#     TOTAL BUFFERED CELLS
---------------------------------------
UCAST       0      0
UCAST       1      0
UCAST       2      0
UCAST       3      0
UCAST       4      0
UCAST       5      0
UCAST       6      0
UCAST       7      0
UCAST       8      0
UCAST       9      0
UCAST       10     0
UCAST       11     1
MCAST       0      0
MCAST       1      0
MCAST       2      0
MCAST       3      0
MCAST       4      0
MCAST       5      0
MCAST       6      0
MCAST       7      0
MCAST       8      0
```

dcb pfc-total-buffer-size

Configure the total buffer size for PFC in kilobytes.

C9000 Series

Syntax

```
dcb pfc-total-buffer-size KB
```

Parameters

KB	Enter a number in the range of 0 to 7787.

Default

The default is 1 KB for S6000 platforms.

Command Modes

CONFIGURATION mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S6000 platform.

Usage Information

Configure the maximum buffer available for PFC traffic. You can choose to increase or decrease the buffer size that is currently allocated in the system by default. However, if you modify the PFC buffer size to be lower than the previously configured PFC buffer size, the system determines whether this reduction in size is valid without disrupting the existing configuration. In such a scenario, you must disable and re-enable DCB. For example, if you

modify the total buffer size to be 4000 KB from the previous size of 5000 KB, an error message is displayed that this reduction cannot be performed owing to existing system configuration because of queues that are being currently processed.

The lossless queue limit per port is validated based on the `dcb pfc-queues` command. PFC queue configuration identifies the maximum number of queues a port can support. Although the queue limit per port is a baseline when dynamic buffering is enabled, the limit per port for queues depends on the availability of the buffer.

Example

```
Dell(conf)#dcb pfc-total-buffer-size  5000
```

```
Dell(conf)#dcb pfc-total-buffer-size  4000
%ERROR: Total pfc buffer size configured cannot accommodate existing buffer
requirement in the system.
```

show running-config dcb-buffer-threshold

Display the DCB buffer threshold details in the running configuration.

C9000 Series

Syntax `show running—config buffer-threshold`

Command Modes EXEC

EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S6000 platform.

Usage Information The following table describes the output fields displayed for the `show running-config dcb-buffer-threshold` command:

Field	Description
Profile name	Name of the DCB buffer threshold profile
Priority	The priority of the queue for which the buffer space settings apply
buffer-size	Ingress buffer size
pause-threshold-value	Buffer limit at which the port sends the pause to peer in KB.
resume-threshold-value	Buffer offset limit at which the port resumes the peer in KB.

The following table describes the output fields displayed for the `show interface pfc buffer-threshold` command:

Field	Description
queue	Number of the queue
lossless	Whether the queue is a lossy or lossless queue for which buffer threshold is configured
buffer-size	Ingress buffer size
pause-threshold-value	Buffer limit at which the port sends the pause to peer in KB.
resume-threshold-value	Buffer offset limit at which the port resumes the peer in KB.
shared threshold weight	Weightage of the priorities on the shared buffer size in the system.

Example

```
Dell#show run buffer-threshold
!
dcb-buffer-threshold test1
pfc priority 0 buffer-size 40
pfc priority 3 buffer-size 50
!
dcb-buffer-threshold test2
pfc priority 0 buffer-size 80 pause-threshold 50
!
dcb-buffer-threshold test3
pfc priority 0 buffer-size 80 pause-threshold 60 resume-threshold 30
```

```
On interface on which PFC is enabled:

Show interface tengigabitethernet 1/1 pfc buffer-threshold
------------------------------------------------------------------------
Queue# Lossless Buffer-size Pause-threshold  Resume-offset Shared threshold
                 (KB)         (KB)              (KB)           weight
------------------------------------------------------------------------
0      No        -              -               -             -
1      No        -              -               -             -
2      Yes       -              20              -             9
3      Yes       52             25              15            0
4      Yes       -              45              25            5
5      No        -              -               -             -
6      No        -              -               -             -
7      No        -              -               -             -
-    Denotes dynamic buffering is enabled in respective queues
```

```
On interface on which PFC is enabled:

Show interface gigabitethernet 1/1 pfc buffer-threshold
------------------------------------------------------------------------
Queue# Lossless Buffer-size Pause-threshold Resume-offset Shared threshold
                 (KB)              (KB)           (KB)        weight
------------------------------------------------------------------------
0      No       -              -               -               -
1      No       -              -               -               -
2      Yes      -              20              -               9
3      Yes      52             25              15              0
4      Yes      -              45              25              5
5      No       -              -               -               -
6      No       -              -               -               -
7      No       -              -               -               -
-    Denotes dynamic buffering is enabled in respective queues
```

```
On interface on which PFC is enabled:
```

```
Show interface tengigabitethernet 1/1/1 pfc buffer-threshold
-------------------------------------------------------------------------
Queue# Lossless Buffer-size Pause-threshold Resume-offset Shared threshold
                  (KB)           (KB)           (KB)          weight
-------------------------------------------------------------------------
0       No       -              -              -              -
1       No       -              -              -              -
2       Yes      -              20             -              9
3       Yes      52             25             15             0
4       Yes      -              45             25             5
5       No       -              -              -              -
6       No       -              -              -              -
7       No       -              -              -              -
-    Denotes dynamic buffering is enabled in respective queues
```

```
On interface in which PFC is not enabled:

Dell#show interface tengigabitethernet 1/20 pfc buffer-threshold
```

```
On interface in which PFC is not enabled:

Dell#show interface gigabitethernet 1/20 pfc buffer-threshold
```

```
On interface in which PFC is not enabled:

Dell#show interface tengigabitethernet 1/20/1 pfc buffer-threshold
```

dcb pfc-queues

Configure the number of PFC queues.

C9000 Series

Syntax `dcb pfc-queues value`

Parameters

value	Enter the number of PFC queues in the range of 0 through 4. The number of ports supported based on lossless queues configured will depend on the buffer.

Default The default number of PFC queues in the system is 2 for S4810 and 1 for S6000 platforms.

Command Modes CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810 and S6000 platforms.

Usage Information You can configure up to a maximum of four lossless (PFC) queues. By configuring four lossless queues, you can configure four different priorities and assign a particular priority to each application that your network is used to process. For example, you can assign a higher priority for time-sensitive applications and a lower priority for other services, such as file transfers. You can configure the amount of buffer space to be allocated for each priority and the pause or resume thresholds for the buffer. This method of configuration enables you to effectively manage and administer the behavior of lossless queues.

Example

```
Dell(conf)#dcb pfc-queues 4
```

dcb {ets | pfc} enable

Enable priority flow control or enhanced transmission selection on interface.

C9000 Series

Syntax

```
dcb {ets | pfc} enable
```

- To disable ETS on interface, use "**no dcb ets enable**" command.
- To disable PFC on interface, use "**no dcb pfc enable**" command.

Defaults

Enable

Command Modes

INTERFACE

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.3 (0.1)	Introduced on S6000, S4810, and S4820T.

Usage Information

PFC and ETS are enabled by default on the interfaces when DCB is globally enabled (refer to dcb enable). In some network topology, you may want to disable PFC on an interface and apply link level flow control; Similarly you may want to disable ETS on an interface and apply QoS bandwidth configurations.

Limitations

- "`dcb-map`" CLI on interface is mutually exclusive to "`no dcb ets enable`" and "`no dcb pfc enable`".
- "`pfc priority`" CLI is mutually exclusive to "`no dcb pfc enable`" command.
- Deprecated CLI "`dcb-policy input`" and "`no dcb pfc enable`" cannot coexist at interface level.
- Deprecated CLI "`dcb-policy output`" and "`no dcb ets enable`" cannot coexist at interface level.

12

Debugging and Diagnostics

Use the debugging and diagnostics commands described in this chapter to troubleshoot switch operation.

This chapter contains the following sections:

- Offline Diagnostic Commands
- Hardware Commands

Topics:

- Offline Diagnostic Commands
- Hardware Commands

Offline Diagnostic Commands

Use the offline diagnostics test suite to isolate faults and debug switch hardware. While tests are running, the system results are saved as a text file in the flash directory: TestReport-*N*.txt , where *N* is 0,1, or 2 for the line-card processor (LP) and 0 for the Control processor (CP) and Route Processor (RP). To display the system results in this text file, use the `show file` command.

Important Points to Remember

- Offline diagnostics can only be run when the unit is offline.
- You can only run offline diagnostics on a unit to which you are connected via the console. In other words, you cannot run diagnostics on a unit to which you are connected to via a stacking link.
- Diagnostic results are printed to the screen. The Dell Networking OS does not write them to memory.
- Diagnostics only test connectivity, not the entire data path.

diag

Run offline diagnostics on all CPUs or on a specified CPU in the switch.

C9000 Series

Syntax

```
diag {cp-unit | linecard | pe [pe-id stack-unit unit-number] | system} }
[alllevels | level0 | level1 | level2] [interactive] [testname name][terminate]
```

Parameters

cp *unit-id*

Enter the `cp unit-id` parameters to run offline diagnostic tests only on the Control Processor CPU. The Control Processor CPU ID is 0.

linecard *slot-id*

Enter the `linecard unit-id` parameters to run offline diagnostic tests only on a specified line card. The linecard slot-id range is from 0 to 11. Each line-card CPU processes packets on the corresponding switch line card; for example, line-card CPU 1 processes packets on line card 1.

pe *pe-id*	Enter the `pe pe-id` parameters to run offline diagnostic tests only on a specified port extender unit. The PE ID range is from 0 to 255. **NOTE: The pe option is only available when the feature extended bridge is enabled.**
stack-unit *unit-number*	Enter the `stack-unit` value to run offline diagnostic test on a specified stack-unit. The stack-unit range is 0 to 7.
alllevels	Enter the keyword `all levels` to run the complete set of offline diagnostic tests.
level0	Enter the keyword `level0` to run Level 0 diagnostics. Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.
level1	Enter the keyword `Level1` to run Level 1 diagnostics. Level 1 diagnostics is a smaller set of diagnostic tests with support for automatic partitioning. They perform status/self test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, EEPROM, and CPLD) wherever possible. There are no tests on 10G links. At this level, ports are shut down automatically.
level2	Enter the keyword `level2` to run Level 2 diagnostics. Level 2 diagnostics are a full set of diagnostic tests with no support for automatic partitioning. Level 2 diagnostics are used primarily for on-board loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations.
interactive	Enter the keyword `interactive` to run offline diagnostics in interactive mode. **NOTE: On a C1048P, interactive diagnostic tests are supported only in standalone mode; they are not supported in stacking mode and only from the PE console.**
testname *name*	Enter the `testname name` parameters to run a specified offline diagnostic test. Enclose the test-case name in double quotes (" "). For example: `diag level1 testname "eepromTest"`.
terminate	Enter the keyword `terminate` to stop the offline diagnostic tests that are running.

Defaults

All offline diagnostic tests are run on all switch CPUs (Control Processor, Route Processor, and line cards).

Command Modes

EXEC Privilege

Usage Information

Before you use this command to run diagnostic test, make sure that the switch is offline (`offline system` command).

You are prompted to reboot when the offline diagnostics complete.

The PE unit goes offline and reboots automatically after the test is completed.

Use the `show diag` command to view a summary of diagnostic information presented for each switch CPU. For PE, this command is used to upload the TestReport from the PE to the C9000 in the `DEFAULT_DIAG_REPORT_DIR`. For example:

```
Dell#pwd flash:/DEFAult_diag_report_dir
```

```
Use the show diag command to upload the diag TestReport as shown below:
Dell#show diag pe 8 stack-unit 0
 % Diag Report file flash:/DEFAULT_DIAG_REPORT_DIR/TestReport-SU-0-
PE-8-20150328_200647.txt copied successfully.

  Dell#dir Directory of flash:/DEFAult_diag_report_dir
   1  drwx       4096   Mar 12 2015 22:53:32 +00:00 .
   2  drwx       4096   Jan 01 1980 00:00:00 +00:00 ..
   3  -rwx       8971   Mar 28 2015 20:06:52 +00:00 TestReport-SU-0-
PE-8-20150328_200647.txt
  flash: 4490649600 bytes total (3658694656 bytes free)
```

At the end of offline diagnostic tests, a test report is generated. The filename of the report is TestReport-{CP/LP/RP}-*N*.txt, where {CP/LP/RP}-*N* identifies the CPU and CPU ID on which the diagnostics were run: Route Processor 0, Control Processor 0, and a line-card CPU {0–2}. The report is stored at flash:// and ramdisk:/diagnostic. Offline diag test reports for port extender (PE) are stored in the following directory: `flash:/default_diag_report_dir`. To view the test report, use the `show file flash://filename` command. A sample *filename* is TestReport-LP-2.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the `verbose` option.
7.7.1.0	Introduced on the S-Series.

Related Commands

offline system— bring a switch offline to run diagnostic tests.

offline linecard

Place the linecard in the offline state in order to run the diagnostics tests.

C9000 Series

Syntax `offline linecard`

Defaults none

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command-Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

A warning message appears when the `offline linecard` command is implemented.

```
Warning - offline of linecard will bring down all the protocols and
the linecard will be operationally down, except for running Diagnostics.
The "reload or reset" command is required for normal operation after the
offline command is issued.
Proceed with Offline [confirm yes/no]:
```

To bring the linecard back to online state, reset the linecard using the `reset linecard` *`slot-id`* command.

Related Commands

diag — run diagnostic tests on an offline switch.

offline system

Place the switch in the offline state in order to run diagnostic tests.

C9000 Series

Syntax `offline system`

Defaults none

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added a warning message to the off-line diagnostic.
7.7.1.0	Introduced on the S-Series.

Usage Information

To run diagnostic tests on an offline switch, use the `diag` command.

The system reboots when offline diagnostics complete. This reboot is an automatic process. A warning message appears when the `offline system` command is implemented.

```
Warning - Diagnostic execution will cause system to reboot after completion of
diags.

Proceed with Offline-Diags [confirm yes/no]:y
```

Related Commands diag — run diagnostic tests on an offline switch.

show diag

Display results of offline diagnostic tests on a switch.

C9000 Series

Syntax

```
show diag {cp unit-id [detail | summary]| pe pe-id stack-unit unit-number}|
information | linecard slot-id [detail | summary]| testcase {cp | pepe-id |
linecard slot-id} }
```

From a **PE console**, use `show diag testcase stack-unit unit number [detail | summary]`

Parameters

cp *unit-id*	Enter the `cp unit-id` parameters to display the results only of the offline diagnostic tests run on the Control Processor CPU. The Control Processor CPU ID is 0.
pe *pe-id*	Enter the `pe pe-id` parameters to display the results only of the offline diagnostic tests run on the Port Extender (PE). The PE ID range is from 0 to 255. **NOTE: The pe option is only available when the feature extended bridge is enabled.**
stack-unit *unit-number*	Enter the `stack–unit unit-number` parameters to display the offline diagnostic test results of a specified stack-unit.
information	Enter the keyword `information` to view the current diag information in the system.
linecard *slot-id*	Enter the `linecard slot-id` parameters to display the results only of the offline diagnostic test run on a specified line card. he range of line-card CPU IDs is from 0 to 11. Each line-card CPU processes packets on the corresponding switch line card; for example, line-card CPU 1 processes packets on line card 1.
summary	Enter the keyword `summary` to display a summary of the offline diagnostic test results.
detail	Enter the keyword `detail` to display detailed information about the offline diagnostic test results.
testcase	Enter the keyword `testcase` to display the diag testcases available for CP, PE, or the Linecard.

Defaults View a summary of the offline diagnostic test results that ran on all CPUs (Control Processor, Route Processor, line cards, and Port Extenders).

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the `verbose` option.
7.7.1.0	Introduced on the S-Series.

Usage Information

Use the `show diag` command to view a summary of diagnostic information presented for each switch CPU. CPU diagnostic results are presented in the following order: Control Processor (CP), line-card processor 0 (LP0), line-card processor 1 (LP1), line-card processor 2 (LP2), and Route Processor (RP).

Example: While offline diagnostics are running on a line card

```
Dell# show diag linecard 0 detail
Diag status of linecard member 0:
---------------------------------

    linecard is currently offline.
    linecard level0 diag issued at Wed Jan 08, 2014 04:39:58 AM.
    Current diag status           : Card diags are in progress.
    Last notification received at Wed Jan 08, 2014 04:40:05 AM
    Last notification message     : Testing ... rtcTest


Dell# show diag linecard 0 summary
Diag status of linecard member 0:
---------------------------------

    linecard is currently offline.
    linecard level0 diag issued at Wed Jan 08, 2014 04:39:57 AM.
    Current diag status           : Card diags are in progress.
    Last notification received at Wed Jan 08, 2014 04:40:04 AM
    Last notification message     : Testing ... rtcTest
```

Example: After offline diagnostics are run on a line card

```
Dell#show file TestReport-LP-0.txt
Called with cpu = 3 slotID = 0


         DELL  DIAGNOSTICS-C9000-CP00  [0]

           CpuType               -- LM
           PPID                  -- CN0CYFF2779314520008
           PPID Rev              -- X00
           Service Tag           -- 11VRG02
           Part Number           -- 0CYFF2
           Part Number Revision  -- X00
           LM CPLD               --  c
           LM extended CPLD      --  5
           SW Version            -- 1-0(0-4079)


           Available free memory: 1,705,611,264 bytes


                   LEVEL 0 DIAGNOSTIC

Starting test: bcm56854AccessTest ......
```

```
+ Access Test for unit 0 : PASSED
bcm56854AccessTest ..................................... PASS
biosVerGetTest ......................................... PASS
boardRevisionTest ...................................... PASS
cpldAccessTest ......................................... PASS
Starting test: CpuGbeLinkStatusTest ......
+ GbE1 Link Status DOWN
+ GbE2 Link Status UP
CpuGbeLinkStatusTest ................................... FAIL
cpuRevisionTest ........................................ PASS
cpuSdramPresenceTest ................................... PASS
cpuSdramSizeTest ....................................... PASS
eepromTest ............................................. PASS
extenderCpldAccessTest ................................. PASS
Starting test: hgLinkStatusTest ......
ERROR: hg port 27 is DOWN
ERROR: hg port 28 is DOWN
ERROR: hg port 29 is DOWN
ERROR: hg port 30 is DOWN
ERROR: hg port 31 is DOWN
ERROR: hg port 32 is DOWN
hgLinkStatusTest ....................................... FAIL
Starting test: i2cTest ......
ERROR: ioctl: "pol3.3V" op(1)=READ WITH STOP bus=4 address=0x57 offset=0x2
length=1
ERROR: ioctl: "SFP2" op(1)=READ WITH STOP bus=11 address=0x50 offset=0 length=1
ERROR: ioctl: "SFP3" op(1)=READ WITH STOP bus=12 address=0x50 offset=0 length=1
ERROR: ioctl: "SFP5" op(1)=READ WITH STOP bus=14 address=0x50 offset=0 length=1
i2cTest ................................................ FAIL
Starting test: opticEepromTest ......
ERROR: optic:9 is not present
ERROR: optic:13 is not present
ERROR: optic:21 is not present
opticEepromTest ........................................ FAIL
opticPhyTest ........................................... PASS
Starting test: opticPresenceTest ......
ERROR: optic:9 is not present
ERROR: optic:13 is not present
ERROR: optic:21 is not present
opticPresenceTest ...................................... FAIL
Starting test: pcieScanTest ......
17 PCI devices installed out of 17
pcieScanTest ........................................... PASS
rtcTest ................................................ PASS
sataSsdTest ............................................ PASS
Starting test: showTemperature ......
        +Board First Thermal Monitor Sensor[0] is 42.0 C
        +Board First Thermal Monitor Sensor[1] is 33.0 C
        +Board First Thermal Monitor Sensor[2] is 34.0 C
        +Board First Thermal Monitor Sensor[3] is 255.0 C
CPU Temp 25 c
DDR Temperature  33 c
showTemperature ........................................ PASS
slotInfoTest ........................................... PASS
Starting test: spiFlashAccessTest ......temperature monitor 0: current= 52.0,
peak= 54.1
temperature monitor 1: current= 52.5, peak= 54.7
temperature monitor 2: current= 53.1, peak= 56.3
temperature monitor 3: current= 52.5, peak= 54.1
temperature monitor 4: current= 54.1, peak= 56.8
temperature monitor 5: current= 54.7, peak= 56.8
temperature monitor 6: current= 55.8, peak= 57.4
temperature monitor 7: current= 56.3, peak= 58.5
temperature monitor 8: current= 56.3, peak= 58.5
average current temperature is  54.1
maximum peak temperature is 58.5
spiFlashAccessTest ..................................... PASS
Starting test: udfLinkStatus ......
ERROR: Unit 0 xe port 25 is DOWN
```

```
udfLinkStatus ............................................... FAIL
xeLinkSpeedTest ............................................. PASS
Starting test: xeLinkStatusTest ......
ERROR: xe port 1 is DOWN
ERROR: xe port 5 is DOWN
ERROR: xe port 9 is DOWN
ERROR: xe port 13 is DOWN
ERROR: xe port 17 is DOWN
ERROR: xe port 21 is DOWN
xeLinkStatusTest ............................................ FAIL


--------- Group Test Statistics ---------
Cpu Name     : CP00
Total        :  24
Passed       :  17
Failed       :   7
Aborted      :   0
Elapsed time : 00H:00M:11S
Stop reason  : after completion
------ Failed tests (level, times) ------
        CpuGbeLinkStatusTest (0, 1)
            hgLinkStatusTest (0, 1)
                     i2cTest (0, 1)
             opticEepromTest (0, 1)
            opticPresenceTest (0, 1)
               udfLinkStatus (0, 1)
             xeLinkStatusTest (0, 1)
```

Example: show diag testcase stack-unit (PE Console)

```
Dell#show diag testcase  stack-unit 1

----------------------------------------    L0    L1    L2    L3    IA
                boardRevision: ALL   RUN   YES    NO    NO    NO    NO
                   cpldAccess: ALL   RUN   YES    NO    NO    NO    NO
             cpuSnakeStackExt: ALL   RUN    NO    NO    NO    NO   YES
                      cpuType: ALL   RUN   YES    NO    NO    NO    NO
                deviceShutPhy: ALL   RUN    NO    NO    NO    NO   YES
                deviceShutPoe: ALL   RUN    NO    NO    NO    NO   YES
        fanControllerSpeedGet: ALL   RUN   YES    NO    NO    NO    NO
                 fanStatusLED: ALL   RUN    NO    NO    NO    NO   YES
             fanStatusMonitor: ALL   RUN   YES    NO    NO    NO    NO
                    fePortLED: ALL   RUN    NO    NO    NO    NO   YES
                flashAccess: ALL   RUN   YES    NO    NO    NO    NO
                    flashRW: ALL   RUN    NO   YES    NO    NO    NO
                gpioAccess: ALL   RUN   YES    NO    NO    NO    NO
       hotswapControllerAccess: ALL   RUN   YES    NO    NO    NO    NO
                     i2cScan: ALL   RUN    NO    NO    NO    NO   YES
                     i2cTool: ALL   RUN    NO    NO    NO    NO   YES
              InterruptStatus: ALL   RUN    NO    NO    NO    NO   YES
                    ixiaSnake: ALL   RUN    NO    NO    NO    NO   YES
                   macAccess: ALL   RUN   YES    NO    NO    NO    NO
                  oneGAccess: ALL   RUN   YES    NO    NO    NO    NO
               oneGPhyExtLink: ALL   RUN    NO   YES    NO    NO    NO
              oneGPhyExtSpeed: ALL   RUN    NO   YES    NO    NO    NO
                    oneGPhyRW: ALL   RUN    NO   YES    NO    NO    NO
        poeControllerPresence: ALL   RUN   YES    NO    NO    NO    NO
              poeControllerRW: ALL   RUN    NO   YES    NO    NO    NO
                   poedetails: ALL   RUN   YES    NO    NO    NO    NO
           poeManagerPresence: ALL   RUN   YES    NO    NO    NO    NO
               poeManagerTemp: ALL   RUN   YES    NO    NO    NO    NO
               poeManagerVolt: ALL   RUN   YES    NO    NO    NO    NO
                      poepLED: ALL   RUN    NO    NO    NO    NO   YES
                     poepLoad: ALL   RUN    NO    NO    NO    NO   YES
                poeUARTStress: ALL   RUN   YES    NO    NO    NO    NO
              powerRailStatus: ALL   RUN   YES    NO    NO    NO    NO
              psuEepromAccess: ALL   RUN   YES    NO    NO    NO    NO
                  psuEepromRW: ALL   RUN    NO   YES    NO    NO    NO
              psuEpsLEDStatus: ALL   RUN    NO    NO    NO    NO   YES
```

```
                psuEpsPresence: ALL    RUN    YES     NO     NO     NO     NO
           psuEpsStatusMonitor: ALL    RUN    YES     NO     NO     NO     NO
             psuFanAirFlowType: ALL    RUN    YES     NO     NO     NO     NO
                  psuFanStatus: ALL    RUN    YES     NO     NO     NO     NO
                  psuInputType: ALL    RUN    YES     NO     NO     NO     NO
                  psuLEDStatus: ALL    RUN     NO     NO     NO     NO    YES
             psuStatusMonitor: ALL    RUN    YES     NO     NO     NO     NO
                      psuTemp: ALL    RUN    YES     NO     NO     NO     NO
                 rtcBattery: ALL    RUN     NO     NO     NO     NO    YES
               rtcFunctional: ALL    RUN     NO     NO     NO     NO    YES
                 rtcPresence: ALL    RUN    YES     NO     NO     NO     NO
                 rtcRollover: ALL    RUN     NO     NO     NO     NO    YES
                       rtcRW: ALL    RUN     NO    YES     NO     NO     NO
           sevendigitStackLED: ALL    RUN     NO     NO     NO     NO    YES
          sfpPlusEepromAccess: ALL    RUN    YES     NO     NO     NO     NO
              sfpPlusEepromRW: ALL    RUN     NO    YES     NO     NO     NO
            sfpPlusPhyExtLink: ALL    RUN     NO    YES     NO     NO     NO
           sfpPlusPhyExtSpeed: ALL    RUN     NO    YES     NO     NO     NO
                 sfpPlusPhyRW: ALL    RUN     NO    YES     NO     NO     NO
              sfpPlusPortLED: ALL    RUN     NO     NO     NO     NO    YES
             sfpPlusPresence: ALL    RUN    YES     NO     NO     NO     NO
                snakeOneGMac: ALL    RUN     NO     NO    YES     NO     NO
                snakeOneGPhy: ALL    RUN     NO     NO    YES     NO     NO
              snakeSfpPlusMac: ALL    RUN     NO     NO    YES     NO     NO
              snakeSfpPlusPhy: ALL    RUN     NO     NO    YES     NO     NO
                snakeStackMac: ALL    RUN     NO     NO    YES     NO     NO
                snakeStackPhy: ALL    RUN     NO     NO    YES     NO     NO
                      stackLED: ALL    RUN     NO     NO     NO     NO    YES
              stackPhyExtLink: ALL    RUN     NO    YES     NO     NO     NO
             stackPhyExtSpeed: ALL    RUN     NO    YES     NO     NO     NO
                   stackPhyRW: ALL    RUN     NO    YES     NO     NO     NO
                   systemInfo: ALL    RUN     NO     NO     NO     NO    YES
                  systemReset: ALL    RUN     NO     NO     NO     NO    YES
              systemStatusLED: ALL    RUN     NO     NO     NO     NO    YES
    systemTempMonitorLEDTest: ALL    RUN     NO     NO     NO     NO    YES
                tsensorAccess: ALL    RUN    YES     NO     NO     NO     NO
                    usbAccess: ALL    RUN    YES     NO     NO     NO     NO
              usbPowerEnable: ALL    RUN    YES     NO     NO     NO     NO
                       usbRW: ALL    RUN     NO    YES     NO     NO     NO
                   usbStatus: ALL    RUN    YES     NO     NO     NO     NO
                watchdogTimer: ALL    RUN     NO     NO     NO     NO    YES
```

show diag information

Display the status of offline diagnostic tests on a switch.

C9000 Series

Syntax

`show diag information`

From a **PE console**, use the `show diag information` command to view the current diag information in the system.

Defaults

None.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the `verbose` option.
7.7.1.0	Introduced on the S-Series.

Usage Information

Use the `show diag information` command to view the progress of offline diagnostics in the system.

Example: Before offline diagnostics are run on a switch

```
Dell#show diag information
Diag information:
Diag software image version:
1-0(0-4079)
------------------------------------------------------------------
  Linecard slot  0:     No card diags executed yet (Card Offline).
  Linecard slot  1:     Not present.
  Linecard slot  2:     No card diags executed yet (Card not Offline).
  Linecard slot  3:     Not present.
  Linecard slot  4:     Not present.
  Linecard slot  5:     No card diags executed yet (Card not Offline).
  Linecard slot  6:     No card diags executed yet (Card not Offline).
  Linecard slot  7:     Not present.
  Linecard slot  8:     Not present.
  Linecard slot  9:     Not present.
  Linecard slot 10:     Not present.
  Linecard slot 11:     No card diags executed yet (Card not Offline).
------------------------------------------------------------------
```

Example: After offline diagnostics are run on a switch

```
Dell#show diag information
Diag information:
Diag software image version:
1-0(0-4079)
------------------------------------------------------------------
  Linecard slot  0:     Card diags are done (Card Offline).
  Linecard slot  1:     Not present.
  Linecard slot  2:     No card diags executed yet (Card not Offline).
  Linecard slot  3:     Not present.
  Linecard slot  4:     Not present.
  Linecard slot  5:     No card diags executed yet (Card not Offline).
  Linecard slot  6:     No card diags executed yet (Card not Offline).
  Linecard slot  7:     Not present.
  Linecard slot  8:     Not present.
  Linecard slot  9:     Not present.
  Linecard slot 10:     Not present.
  Linecard slot 11:     No card diags executed yet (Card not Offline).
------------------------------------------------------------------
```

Example: PE Console

```
 Dell#show diag information
Diag information:
Diag software image version:
1-0(0-4092)
------------------------------------------------------------------
  stack-unit Member  0:     Not present.
  stack-unit Member  1:     No Unit diags executed yet (stack-unit not
Offline).
```

```
  stack-unit Member  2:     Not present.
  stack-unit Member  3:     Not present.
  stack-unit Member  4:     Not present.
  stack-unit Member  5:     Not present.
  stack-unit Member  6:     Not present.
  stack-unit Member  7:     Not present.
-------------------------------------------------------------------
```

show diag testcase

Display the offline diagnostic tests available for the CPUs at each level.

C9000 Series

Syntax

`show diag testcase {cp |linecard | pe` *`pe-id`* `[alllevels | level0 | level1 | level2]}`

From a **PE console**, use `show diag testcase {stack-unit` *`unit-number`* `[alllevels | interactive | level0 | level1 | level2]}`

Parameters

cp *unit-id*	Enter the `cp` *`unit-id`* parameters to display only the offline diagnostic tests available on the Control Processor CPU. The Control Processor CPU ID is 0.
pe	Enter the`pe` *`pe-id`* parameters to display only the offline diagnostic test available on the port extender (PE).
stack-unit *unit-number*	Enter the`stack-unit` *`unit number`* parameters to display only the offline diagnostic test available on the specified stack unit. The range is from 0 to 7.
linecard *slot-id*	Enter the `linecard` *`slot-id`* parameters to display only the offline diagnostic tests available for a specified line card. The range of line-card CPU IDs is from 0 to 11. Each line-card CPU processes packets on the corresponding switch line card; for example, line-card CPU 1 processes packets on line card 1.
alllevels	Enter the keyword `alllevels` to display the complete set of offline diagnostic tests.
interactive	Enter the keyword `interactive` to display interactive diag testcases.
level0	Enter the keyword `level0` to display only the Level 0 diagnostic tests. Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.
level1	Enter the keyword `level1` to display only the Level 1 diagnostic tests. Level 1 diagnostics is a smaller set of diagnostic tests with support for automatic partitioning. They perform status/self test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, EEPROM, and CPLD) wherever possible. There are no tests on 10G links. At this level, ports are shut down automatically.
level2	Enter the keyword `level2` to display only the Level 2 diagnostic tests. Level 2 diagnostics are a full set of diagnostic tests with no support for automatic partitioning. Level 2 diagnostics are used primarily for on-board loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode

and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations.

Defaults Display the complete set of offline diagnostic tests available at all levels.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the `verbose` option.
7.7.1.0	Introduced on the S-Series.

Usage Information Offline diagnostics tests are grouped into three levels:

- Level 0 — Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.
- Level 1 — A smaller set of diagnostic tests. Level 1 diagnostics perform status/self-test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, or EEPROM) wherever possible.
- Level 2 — The full set of diagnostic tests. Level 2 diagnostics are used primarily for on-board Loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations.

Example

```
Dell#sho diag testcase linecard 0

-----------------------------------------    L0    L1    L2    L3    IA
             bcm56854AccessTest: ALL   RUN   YES    NO    NO    NO    NO
                 biosVerGetTest: ALL   RUN   YES    NO    NO    NO    NO
              boardRevisionTest: ALL   RUN   YES    NO    NO    NO    NO
                 cpldAccessTest: ALL   RUN   YES    NO    NO    NO    NO
           CpuGbeLinkStatusTest: ALL   RUN   YES    NO    NO    NO    NO
                cpuRevisionTest: ALL   RUN   YES    NO    NO    NO    NO
           cpuSdramPresenceTest: ALL   RUN   YES    NO    NO    NO    NO
               cpuSdramSizeTest: ALL   RUN   YES    NO    NO    NO    NO
                    eepromTest: ALL   RUN   YES    NO    NO    NO    NO
         extenderCpldAccessTest: ALL   RUN   YES    NO    NO    NO    NO
               hgLinkStatusTest: ALL   RUN   YES    NO    NO    NO    NO
                        i2cTest: ALL   RUN   YES   YES    NO    NO    NO
                 ipcTrafficTest: ALL   RUN    NO    NO   YES    NO    NO
               opticEepromTest: ALL   RUN   YES    NO    NO    NO    NO
                  opticPhyTest: ALL   RUN   YES   YES    NO    NO    NO
              opticPresenceTest: ALL   RUN   YES    NO    NO    NO    NO
                   pcieScanTest: ALL   RUN   YES    NO    NO    NO    NO
                        rtcTest: ALL   RUN   YES   YES    NO    NO    NO
                  sataSsdTest: ALL   RUN   YES   YES    NO    NO    NO
          showOpticsTemperature: ALL   RUN    NO    NO    NO    NO   YES
                showTemperature: ALL   RUN   YES    NO    NO    NO    NO
```

```
                  slotInfoTest: ALL   RUN   YES    NO    NO    NO    NO
              spiFlashAccessTest: ALL   RUN   YES    NO    NO    NO    NO
   ssdFlashFileSystemStressTest: ALL   RUN    NO   YES    NO    NO    NO
                udfLinkStatus: ALL   RUN   YES    NO    NO    NO    NO
             xeLinkSpeedTest: ALL   RUN   YES    NO    NO    NO    NO
            xeLinkStatusTest: ALL   RUN   YES    NO    NO    NO    NO
```

Example (pe)

```
Dell#show diag testcase pe 10 alllevels

-----------------------------------------    L0    L1    L2    L3    IA
                boardRevision: ALL   RUN   YES    NO    NO    NO    NO
                   cpldAccess: ALL   RUN   YES    NO    NO    NO    NO
                      cpuType: ALL   RUN   YES    NO    NO    NO    NO
                deviceShutPhy: ALL   RUN    NO    NO    NO    NO   YES
                deviceShutPoe: ALL   RUN    NO    NO    NO    NO   YES
         fanControllerSpeedGet: ALL   RUN   YES    NO    NO    NO    NO
                   fanStatusLED: ALL   RUN    NO    NO    NO    NO   YES
              fanStatusMonitor: ALL   RUN   YES    NO    NO    NO    NO
                     fePortLED: ALL   RUN    NO    NO    NO    NO   YES
                  flashAccess: ALL   RUN   YES    NO    NO    NO    NO
                      flashRW: ALL   RUN    NO   YES    NO    NO    NO
                   gpioAccess: ALL   RUN   YES    NO    NO    NO    NO
       hotswapControllerAccess: ALL   RUN   YES    NO    NO    NO    NO
                       i2cScan: ALL   RUN    NO    NO    NO    NO   YES
                       i2cTool: ALL   RUN    NO    NO    NO    NO   YES
               InterruptStatus: ALL   RUN    NO    NO    NO    NO   YES
                     ixiaSnake: ALL   RUN    NO    NO    NO    NO   YES
                    macAccess: ALL   RUN   YES    NO    NO    NO    NO
                   oneGAccess: ALL   RUN   YES    NO    NO    NO    NO
                oneGPhyExtLink: ALL   RUN    NO   YES    NO    NO    NO
               oneGPhyExtSpeed: ALL   RUN    NO   YES    NO    NO    NO
                     oneGPhyRW: ALL   RUN    NO   YES    NO    NO    NO
          poeControllerPresence: ALL   RUN   YES    NO    NO    NO    NO
                poeControllerRW: ALL   RUN    NO   YES    NO    NO    NO
                    poedetails: ALL   RUN   YES    NO    NO    NO    NO
             poeManagerPresence: ALL   RUN   YES    NO    NO    NO    NO
                 poeManagerTemp: ALL   RUN   YES    NO    NO    NO    NO
                 poeManagerVolt: ALL   RUN   YES    NO    NO    NO    NO
                        poepLED: ALL   RUN    NO    NO    NO    NO   YES
                       poepLoad: ALL   RUN    NO    NO    NO    NO   YES
                  poeUARTStress: ALL   RUN   YES    NO    NO    NO    NO
                powerRailStatus: ALL   RUN   YES    NO    NO    NO    NO
                psuEepromAccess: ALL   RUN   YES    NO    NO    NO    NO
                    psuEepromRW: ALL   RUN    NO   YES    NO    NO    NO
                psuEpsLEDStatus: ALL   RUN    NO    NO    NO    NO   YES
                 psuEpsPresence: ALL   RUN   YES    NO    NO    NO    NO
            psuEpsStatusMonitor: ALL   RUN   YES    NO    NO    NO    NO
              psuFanAirFlowType: ALL   RUN   YES    NO    NO    NO    NO
                   psuFanStatus: ALL   RUN   YES    NO    NO    NO    NO
                   psuInputType: ALL   RUN   YES    NO    NO    NO    NO
                   psuLEDStatus: ALL   RUN    NO    NO    NO    NO   YES
              psuStatusMonitor: ALL   RUN   YES    NO    NO    NO    NO
                       psuTemp: ALL   RUN   YES    NO    NO    NO    NO
                   rtcBattery: ALL   RUN    NO    NO    NO    NO   YES
                rtcFunctional: ALL   RUN    NO    NO    NO    NO   YES
                  rtcPresence: ALL   RUN   YES    NO    NO    NO    NO
                  rtcRollover: ALL   RUN    NO    NO    NO    NO   YES
                        rtcRW: ALL   RUN    NO   YES    NO    NO    NO
            sevendigitStackLED: ALL   RUN    NO    NO    NO    NO   YES
           sfpPlusEepromAccess: ALL   RUN   YES    NO    NO    NO    NO
               sfpPlusEepromRW: ALL   RUN    NO   YES    NO    NO    NO
             sfpPlusPhyExtLink: ALL   RUN    NO   YES    NO    NO    NO
            sfpPlusPhyExtSpeed: ALL   RUN    NO   YES    NO    NO    NO
                  sfpPlusPhyRW: ALL   RUN    NO   YES    NO    NO    NO
              sfpPlusPresence: ALL   RUN   YES    NO    NO    NO    NO
                 snakeOneGMac: ALL   RUN    NO    NO   YES    NO    NO
                 snakeOneGPhy: ALL   RUN    NO    NO   YES    NO    NO
```

```
                snakeSfpPlusMac: ALL   RUN    NO    NO   YES    NO    NO
                snakeSfpPlusPhy: ALL   RUN    NO    NO   YES    NO    NO
                  snakeStackMac: ALL   RUN    NO    NO   YES    NO    NO
                  snakeStackPhy: ALL   RUN    NO    NO   YES    NO    NO
                        stackLED: ALL   RUN    NO    NO    NO    NO   YES
                stackPhyExtLink: ALL   RUN    NO   YES    NO    NO    NO
               stackPhyExtSpeed: ALL   RUN    NO   YES    NO    NO    NO
                     stackPhyRW: ALL   RUN    NO   YES    NO    NO    NO
                     systemInfo: ALL   RUN    NO    NO    NO    NO   YES
                    systemReset: ALL   RUN    NO    NO    NO    NO   YES
                systemStatusLED: ALL   RUN    NO    NO    NO    NO   YES
      systemTempMonitorLEDTest: ALL   RUN    NO    NO    NO    NO   YES
                tsensorAccess: ALL   RUN   YES    NO    NO    NO    NO
                    usbAccess: ALL   RUN   YES    NO    NO    NO    NO
                usbPowerEnable: ALL   RUN   YES    NO    NO    NO    NO
                         usbRW: ALL   RUN    NO   YES    NO    NO    NO
                    usbStatus: ALL   RUN   YES    NO    NO    NO    NO
                watchdogTimer: ALL   RUN    NO    NO    NO    NO   YES
```

Example (PE Console)

```
Dell#show diag testcase stack-unit 1 alllevels

-----------------------------------------    L0    L1    L2    L3    IA
                  boardRevision: ALL   RUN   YES    NO    NO    NO    NO
                     cpldAccess: ALL   RUN   YES    NO    NO    NO    NO
               cpuSnakeStackExt: ALL   RUN    NO    NO    NO    NO   YES
                        cpuType: ALL   RUN   YES    NO    NO    NO    NO
                  deviceShutPhy: ALL   RUN    NO    NO    NO    NO   YES
                  deviceShutPoe: ALL   RUN    NO    NO    NO    NO   YES
         fanControllerSpeedGet: ALL   RUN   YES    NO    NO    NO    NO
                   fanStatusLED: ALL   RUN    NO    NO    NO    NO   YES
               fanStatusMonitor: ALL   RUN   YES    NO    NO    NO    NO
                      fePortLED: ALL   RUN    NO    NO    NO    NO   YES
                    flashAccess: ALL   RUN   YES    NO    NO    NO    NO
                         flashRW: ALL   RUN    NO   YES    NO    NO    NO
                    gpioAccess: ALL   RUN   YES    NO    NO    NO    NO
       hotswapControllerAccess: ALL   RUN   YES    NO    NO    NO    NO
                        i2cScan: ALL   RUN    NO    NO    NO    NO   YES
                        i2cTool: ALL   RUN    NO    NO    NO    NO   YES
                InterruptStatus: ALL   RUN    NO    NO    NO    NO   YES
                      ixiaSnake: ALL   RUN    NO    NO    NO    NO   YES
                     macAccess: ALL   RUN   YES    NO    NO    NO    NO
                    oneGAccess: ALL   RUN   YES    NO    NO    NO    NO
                 oneGPhyExtLink: ALL   RUN    NO   YES    NO    NO    NO
                oneGPhyExtSpeed: ALL   RUN    NO   YES    NO    NO    NO
                      oneGPhyRW: ALL   RUN    NO   YES    NO    NO    NO
          poeControllerPresence: ALL   RUN   YES    NO    NO    NO    NO
                poeControllerRW: ALL   RUN    NO   YES    NO    NO    NO
                     poedetails: ALL   RUN   YES    NO    NO    NO    NO
             poeManagerPresence: ALL   RUN   YES    NO    NO    NO    NO
                 poeManagerTemp: ALL   RUN   YES    NO    NO    NO    NO
                 poeManagerVolt: ALL   RUN   YES    NO    NO    NO    NO
                        poepLED: ALL   RUN    NO    NO    NO    NO   YES
                       poepLoad: ALL   RUN    NO    NO    NO    NO   YES
                  poeUARTStress: ALL   RUN   YES    NO    NO    NO    NO
                powerRailStatus: ALL   RUN   YES    NO    NO    NO    NO
                psuEepromAccess: ALL   RUN   YES    NO    NO    NO    NO
                    psuEepromRW: ALL   RUN    NO   YES    NO    NO    NO
                psuEpsLEDStatus: ALL   RUN    NO    NO    NO    NO   YES
                 psuEpsPresence: ALL   RUN   YES    NO    NO    NO    NO
              psuEpsStatusMonitor: ALL   RUN   YES    NO    NO    NO    NO
                psuFanAirFlowType: ALL   RUN   YES    NO    NO    NO    NO
                     psuFanStatus: ALL   RUN   YES    NO    NO    NO    NO
                     psuInputType: ALL   RUN   YES    NO    NO    NO    NO
                     psuLEDStatus: ALL   RUN    NO    NO    NO    NO   YES
                psuStatusMonitor: ALL   RUN   YES    NO    NO    NO    NO
                         psuTemp: ALL   RUN   YES    NO    NO    NO    NO
                      rtcBattery: ALL   RUN    NO    NO    NO    NO   YES
                   rtcFunctional: ALL   RUN    NO    NO    NO    NO   YES
```

```
                    rtcPresence: ALL    RUN    YES     NO     NO     NO     NO
                    rtcRollover: ALL    RUN     NO     NO     NO     NO    YES
                          rtcRW: ALL    RUN     NO    YES     NO     NO     NO
             sevendigitStackLED: ALL    RUN     NO     NO     NO     NO    YES
           sfpPlusEepromAccess: ALL    RUN    YES     NO     NO     NO     NO
               sfpPlusEepromRW: ALL    RUN     NO    YES     NO     NO     NO
             sfpPlusPhyExtLink: ALL    RUN     NO    YES     NO     NO     NO
            sfpPlusPhyExtSpeed: ALL    RUN     NO    YES     NO     NO     NO
                  sfpPlusPhyRW: ALL    RUN     NO    YES     NO     NO     NO
                sfpPlusPortLED: ALL    RUN     NO     NO     NO     NO    YES
              sfpPlusPresence: ALL    RUN    YES     NO     NO     NO     NO
                 snakeOneGMac: ALL    RUN     NO     NO    YES     NO     NO
                 snakeOneGPhy: ALL    RUN     NO     NO    YES     NO     NO
              snakeSfpPlusMac: ALL    RUN     NO     NO    YES     NO     NO
              snakeSfpPlusPhy: ALL    RUN     NO     NO    YES     NO     NO
                snakeStackMac: ALL    RUN     NO     NO    YES     NO     NO
                snakeStackPhy: ALL    RUN     NO     NO    YES     NO     NO
                      stackLED: ALL    RUN     NO     NO     NO     NO    YES
              stackPhyExtLink: ALL    RUN     NO    YES     NO     NO     NO
             stackPhyExtSpeed: ALL    RUN     NO    YES     NO     NO     NO
                   stackPhyRW: ALL    RUN     NO    YES     NO     NO     NO
                   systemInfo: ALL    RUN     NO     NO     NO     NO    YES
                  systemReset: ALL    RUN     NO     NO     NO     NO    YES
               systemStatusLED: ALL    RUN     NO     NO     NO     NO    YES
     systemTempMonitorLEDTest: ALL    RUN     NO     NO     NO     NO    YES
                 tsensorAccess: ALL    RUN    YES     NO     NO     NO     NO
                     usbAccess: ALL    RUN    YES     NO     NO     NO     NO
              usbPowerEnable: ALL    RUN    YES     NO     NO     NO     NO
                       usbRW: ALL    RUN     NO    YES     NO     NO     NO
                   usbStatus: ALL    RUN    YES     NO     NO     NO     NO
                watchdogTimer: ALL    RUN     NO     NO     NO     NO    YES
```

Hardware Commands

The hardware commands supported on the switch allow you to display information from a hardware sub-component or ASIC.

clear control-traffic

Clear control-traffic statistics from the CPU.

C9000 Series

Syntax `clear control-traffic {all | cp-switch | linecard` *`slot-id`* `portset` *`port-pipe`*`} counters`

Parameters

cp-switch	Enter the keyword `cp-switch` to clear the counters for control traffic on the control plane.
linecard *slot-id* **portset** *port-pipe*	Enter the slot ID and port pipe to clear the counters for control traffic on a specified switch line card and port set. The range of slot IDs is from 0 to 2. The range of port-pipe numbers is: 0 to 2 on line card 0 and 0 to 3 on line cards 1 and 2.
all	Enter the keyword `all` to clear control-traffic statistics on the control plane and all line cards.

Defaults None.

Command Modes EXEC Privilege

Example

```
Dell# clear control-traffic cp-switch counters
```

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the ES-Series.

clear hardware

Clear statistics from a specified hardware component.

C9000 Series

Syntax

```
clear hardware {cp {cpu {data-plane | i2c statistics | sata-interface}} | cp-switch {counters} | linecard slot-id {counters | cpu {data-plane | i2c | sata-interface} statistics} | hg-stats| unit unit-num {counters} | party-bus {counters} | pe pe-id stack-unit unit-number {counters | cpu | stack—port | unit} | rp {cpu {data-plane | i2c | sata-interface} statistics} | sfm sfm-unit-num {counters}}
```

Parameters

cp Enter the keywords `cp` with a command option to clear the hardware statistics for the Control Processor. The command options are:

- `cpu data-plane statistics`: Clears data-plane statistics, including the high-Gigabit Ethernet (HiGig) port statistics with input/output counters to which the stacking module is connected.
- `cpu i2c statistics`: Clears active i2c-address statistics.
- `cpu sata-interface statistics`: Clears sata-interface error counter statistics.

cp-switch Enter the keyword `cp-switch` with a command option to clear the hardware statistics for control-plane and protocol control traffic. The command options are:

- `counters`: Clears the counters for control-plane and protocol control packets to troubleshoot an error condition.

linecard *slot-id* Enter the `linecard slot-id` parameters with a command option to clear the hardware statistics for a specified switch line card. The range of slot IDs is from 0 to 11. The command options are:

- `counters`: Clears traffic counters on line-card ports.

- `cpu data-plane statistics`: Clears data-plane statistics, including the HiGig port statistics with input/output counters to which the stacking module is connected.
- `cpu i2c statistics` : Clears active i2c-address statistics.
- `cpu sata-interface statistics`: Clears sata-interface error counter statistics.

unit *unit-num*

Enter the `unit` *`unit-num`* parameters with a command option to clear hardware statistics for a specified NPU. The range of NPU numbers is 0 to 3. The command options are:

- `counters`: Clears the packets counters.

party-bus

Enter the keyword `party-bus` with a command option to clear hardware statistics for the party bus that links the switch CPUs. The command options are:

- `port` *`port-num`* `statistics`: Clears statistics on a specified party-bus internal port.
- `port all`: Clear statistics on all party-bus internal ports.

pe *pe-id*

Enter the keyword `pe` with a port extender (PE) ID to clear hardware statistics for a specified port extender. The PE ID range is from 0 to 255.

NOTE: The pe option is only visible when the extended bridge feature is enabled.

stack-unit *unit-number*

Enter the keyword `stack-unit` with a stack unit number to clear hardware statistics for a specified stack-unit number. The stack-unit number range is from 0 to 7.

rp

Enter the keyword `rp` with a command option to clear hardware statistics for the Route Processor. The command options are:

- `cpu data-plane statistics`: Clears data-plane statistics, including the HiGig port statistics with input/output counters.
- `cpu i2c statistics`: Clears active i2c-address statistics.
- `cpu sata-interface statistics`: Clears sata-interface error counter statistics.

sfm *sfm-unit-num*

Enter the keyword `sfm` with a Switch Fabric Module (SFM) unit number and a command option to clear hardware statistics from the specified SFM. The range of SFM unit numbers is from 0 to 5. The command options are:

- `counters`: Clears the traffic counters.

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.0	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Related Commands show hardware — displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

clear hardware system-flow

Clear system-flow statistics from a specified line card.

C9000 Series

Syntax `clear hardware system-flow {cp-switch | linecard slot-id | pe pe-id stack-unit unit-number} [port-set port-pipe counters]`

Parameters

linecard *slot-id*	Enter the `linecard slot-id` parameters to identify the line card on which you want to clear system-flow statistics. The range of slot IDs is from 0 to 11.
pe *pe-id*	Enter the `pe pe-id` parameters to specify the port extender ID for which you want to clear system-flow statistics. **NOTE: The pe option is only visible when the extended bridge feature is enabled.**
stack-unit *unit-number*	Enter the `stack-unit unit-number` parameters to specify the stack-unit for which you want to clear system-flow statistics.
port-set *port-pipe* counters	Enter the keywords `port-set` along with a port-pipe number, then the keyword counters to clear the system-flow counters on the selected port-pipe. The range of port-pipe numbers is: 0 to 2 on line card 0 and 0 to 3 on line cards 1 and 2.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.8.1.0	Introduced on the S-Series.

Related Commands show hardware — displays the data plane or management plane input and output statistics for a specified hardware component.

remote-exec

Debug and troubleshoot switch hardware using remote commands.

⚠ | **WARNING: Use the `remote-exec` command only with the guidance of an engineer from Dell Networking Technical Support.**

C9000 Series

Syntax `remote-exec {cp | rp | linecard slot-id} hw-command`

Parameters

cp	Enter the keyword `cp` to troubleshoot Control Processor CPU operation.
rp	Enter the keyword `rp` to troubleshoot Route Processor CPU operation.
linecard *slot-id*	Enter the `linecard slot-id` to troubleshoot line-card CPU operation. The range of line-card slot IDs is from 0 to 11. Each line-card CPU processes packets on the corresponding line card on your switch.
hw-command	Enter the debug command that Dell Networking Technical Support gives you.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Modified the `drops` keyword range, unit keyword `range` and added the `buffer` and `cpu management statistics` options.
8.3.19.0	Introduced on the S4820T.
8.3.11.5	Added i2c statistics and sata-interfaces statistics.
8.3.11.4	Added user port information.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.7.1.0	Introduced on the S-Series.

Usage Information Use the `remote-exec` command to remotely execute a command on the Route Processor and line-card (LP) processor from the Control Processor.

Related Commands show hardware — displays information on hardware components.

show hardware

Display input and output traffic statistics and other operational information about a specified hardware component.

C9000 Series

Syntax

```
show hardware {cp {cpu {data-plane | i2c | management| sata-interface}}

buffer-stats-snapshots {resource interface interface}

cp-switch {counters | details | drops | port-stats |register | table-dump}|

forwarding-table mode

linecard slot-id {buffer {total-buffer | unit unit-num [port port-num [queue
queue-num]]} |

pe pe-id stack-unit unit number {cpu | drops | stack-port | unit}

cpu {data-plane | i2c | management | sata-interface} statistics |

drops {unit unit-num {port {port-num | port-range}} |

user-port {user-port-num | port-range}} |

unit unit-num {counters | details | ipmc-replication | port-stats | register |
table-dump} |

bp-link-map | bp-link-state | higig unit unit-num [port port-num]}

party-bus {port port-num statistics | all}

rp {cpu {data-plane | i2c | management | sata-interface} statistics} |

sfm sfm-unit-num {buffer {total-buffer | unit unit-num {port | total-buffer}} |
counters | details| drops | port-stats | register | table-dump}}

system {bp-link-state | linkId range}
```

Parameters

cp Enter the keywords `cp` with a command option to display hardware statistics from the Control Processor. The command options are:

- `cpu data-plane`: Displays data-plane statistics, including the HiGig port statistics with input/output counters to which the stacking module is connected.

- `cpu i2c`: Displays active i2c-interface statistics.
- `cpu management`: Displays management port counters.
- `cpu sata-interface`: Displays sata-interface error counter-statistics.

cp-switch

Enter the keyword `cp-switch` with a command option to display hardware statistics for control-plane and protocol control traffic. The command options are:

- `counters`: Displays the counters for control-plane and protocol control packets to troubleshoot an error condition.
- `details`: Displays more detailed information on control-plane and protocol control packet statistics.
- `drops`: Displays the number of internal drops of control-plane and protocol control packets.
- `port-stats`: Displays status about why a control-plane internal port is not brought up to register level. You can use the `detail` option to display the port-statistics in details.
- `register`: Displays internal control-plane registers.
- `table-dump`: Displays the tables from the bShell.

forwarding-table mode

Enter the keyword `forwarding—table mode` to display the statistics related to forwarding table.

linecard *slot-id*

Enter the `linecard` *`slot-id`* parameters with a command option to display hardware statistics from the specified line-card ports. The range of line-card slot IDs is from 0 to 2. The command options are:

- `buffer total-buffer`: Displays the total number of buffers allocated for a specified line card.
- `buffer unit` *`unit-num`* `port statistics`: Displays the number of buffers allocated for a specified NPU. The range of port-pipe unit numbers is 0–3.
- `buffer unit` *`unit-num`* `total-buffer` : Displays the number of buffers allocated for a specified NPU. The range of NPU numbers is 0–3.
- `cpu data-plane statistics`: Displays data-plane statistics, including the HiGig port statistics with input/output counters to which the stacking module is connected.
- `cpu i2c statistics`: Displays active i2c-address statistics.
- `cpu management statistics`: Displays management port counters for a specified line card.
- `cpu sata-interface statistics`: Displays sata-interface error counter-statistics.
- `drops unit` *`unit-num`* `{port {`*`port-num`* `| range}`: Displays the number of dropped packets on the ports of a specified line-card.
- `user-port {`*`user-port-num`* `|` *`port-range`*`}`: Displays statistics on a specified line-card port or range of ports.
- `unit` *`unit-num`* `{counters | details | ipmc-replication | port-stats | register | table-dump}`: Displays statistics on a specified NPU. The command options are:
  - `counters`: Displays the traffic counters.
  - `details`: Displays more detailed hardware information.
  - `ipmc-replication`: Displays the multicast IPMC replication table from the bShell.
  - `port-stats`: Displays the internal statistics on a per-port basis.
  - `register`: Displays the line-card internal registers.
  - `table-dump`: Displays the tables from the bShell.

- `bp-link-map`: Displays the backplane links (between leaf/port and spine/fabric) on a specified line card.
- `bp-link-state`: Displays the status of the backplane links on a specified line card.
- `hg-stats unit` *`unit-num`* `port` *`port-num`*: Displays input and output statistics for a HiGig port (NPU port number) on a specified line card.
- `fpga registers` Display the statistics from the FPGA registers.

pe *pe-id* **stack unit** *unit-number*

Enter `pe` *`pe-id`* `stack-unit` *`unit number`* parameters with a command option to display hardware statistics from the specified port extender (PE) and stack-unit. The port extender ID range is from 0 to 255 and the stack-unit ID range is from 0 to 7. The command options are:

- `cpu data-plane statistics`: Displays data-plane statistics, including the`bc pci` driver statistics for the device.
- `drops unit` *`unit number`* `[user—port {port {`*`port-num`* `| range}]`: Displays the number of internal drops of control-plane and protocol control packets on the port specified. User port range is 1–51.
- `stack-port` Displays traffic statistics for the stacking ports on a specified PE.
- `unit` *unit-number* to view with the following options:
  - `counters`: Displays the traffic counters.
  - `details`: Displays more detailed hardware information.
  - `port-stats`: Displays the internal statistics on a per-port basis.
  - `register`: Displays the internal registers.
  - `table-dump`: Displays the tables from the bShell.

party-bus

Enter the keyword `party-bus` with a command option to display hardware statistics from the party bus that links the switch CPUs. The command options are:

- `port` *`port-num`* `statistics`: Displays statistics on a specified party-bus internal port.
- `port all`: Displays statistics on all party-bus internal ports.

rp

Enter the keyword `rp` with a command option to display hardware statistics from the Route Processor. The command options are:

- `cpu data-plane statistics`: Displays data-plane statistics, including the HiGig port statistics with input/output counters to which the stacking module is connected.
- `cpu i2c statistics`: Displays active i2c-address statistics.
- `cpu management statistics`: Displays management port counters.
- `cpu sata-interface statistics`: Displays sata-interface error counter-statistics.

sfm *sfm-unit-num*

Enter the keyword `sfm` with a Switch Fabric Module (SFM) unit number and a command option to display hardware statistics from the specified SFM on the switch. The range of SFM unit numbers is from 0 to 5. The command options are:

- `buffer {total-buffer | unit` *`unit-num`* `{port port-num | total-buffer}`: Displays buffer statistics from the total SFM buffer or from a specified SFM unit. The range of SFM unit ID numbers is from 0 to 5. The range of SFM unit ports is from 1 to 4096.
- `counters`: Displays the counters for SFM traffic to troubleshoot an error condition.
- `details`: Displays more detailed information on control-plane and protocol control packet statistics.

- `drops`: Displays the number of internal drops on the specified SFM unit.
- `port-stats`: Displays status about why an SFM port is not brought up to register level.
- `register`: Displays the internal registers for each switch fabric.
- `table-dump`: Displays the tables from the bShell.

system Enter the keyword `system` to display the current status of the system hardware. The command options are:

- `system {bp-link-state}`: Displays the statistics related to the backplane link state bit map.
- `system {bp-link-state linKId range}`: Displays the status of the specified link. LinKId range for the system is from 0 to 155.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Modified the `drops` keyword range, unit keyword `range` and added the `buffer` and `cpu management statistics` options.
8.3.19.0	Introduced on the S4820T.
8.3.11.5	Added i2c statistics and sata-interfaces statistics.
8.3.11.4	Added user port information.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Modified the `stack-port` keyword range expanded from 49-52 to 0-52; output modified for the `cpu data-plane statistics` option; the following options were added: `drops [unit 0-1 [port 0-27]]` and `unit 0-1 {counters | details | port-stats [detail] | register}`
7.7.1.0	Introduced on the S-Series.

Example (Linecard CPU Dataplane: Statistics)

```
Dell#show hardware linecard 2 cpu data-plane statistics

HANSKVILLE Mib Counters:
TR 64 byte frames = 3
TR 127 byte frames = 358
TR 255 byte frames = 1363
TR 511 byte frames = 1934
TR 1023 byte frames = 18
TR MAX Byte frames = 6202
```

```
TR MGV Frames = 0
Bytes Transmitted = 0
Frames Transmitted = 9878
Mcast Frames Transmitted = 0
Bcast Frames Transmitted = 4
Pause Frames Transmitted = 0
Deferred Transmits = 0
Excessive Deferred Transmits = 0
TX single collisions = 0
TX multiple collisions = 0
TX late collisions = 0
TX Excessive collisions = 0
TX total collisions = 0
TX Drops = 0
TX Jabber = 0
TX FCS errors = 0
TX Control frames = 0
TX oversize frames = 0
TX undersize frames = 0
TX fragments = 0
Bytes received = 0
Frames received = 2868
Bcast frames recvd = 24
Mcast frames recvd = 0
Control frames received = 0
Pause frames received = 0
FCS Errors = 0
Alignment errors = 0
Undersize frames recvd = 0
Oversize frames recvd = 0
Fragments = 0
Jabber = 0
Dropped Frames = 0
Under/oversized frames = 0
FLR frames = 0
RCDE frames = 0
RCSE frames = 0
```

Example (Party-Bus Port: Statistics)

```
Dell#show hardware party-bus port 0 statistics

Party Bus Transmit Counters for port 0:
Tx Octets = 231162055
Tx Drop Packets = 0
tx_q0_pkts = 303459
tx_q1_pkts = 0
tx_q2_pkts = 0
tx_q3_pkts = 0
tx_q4_pkts = 0
tx_q5_pkts = 0
tx_broad_pkts = 6178
tx_multi_pkts = 852
tx_uni_pkts = 296429
tx_pause_pkts = 0
tx_cols = 0
tx_single_cols = 0
tx_multi_cols = 0
tx_late_cols = 0
tx_excess_cols = 0
tx_deferred = 0
tx_discarded = 0
Party Bus Receive Counters for port 0:
Rx Octets = 219885483
Rx Undersize Packets = 0
Rx Oversize Packets = 0
Rx Pause Packets = 0
Rx 64 Octet Packets = 115814
Rx 65to127octets Packets = 13278
Rx 128to255octets Packets = 523
```

```
Rx 256to511octets Packets = 3382
Rx 512to1023octets Packets = 2530
Rx 1024toMaxoctets Packets = 141767
Rx Jabbers = 0
Rx align errors = 0
Rx fcs errors = 0
Rx good octets = 219885483
Rx Drop pkts = 0
Rx Unicast Packets = 277279
Rx Multicast Packets = 0
Rx Broadcast Packets = 15
Rx Source Address Changes = 1
Rx Fragments = 0
Rx Jumbo Packets = 0
Rx Symbol Errros = 0
Rx In Range Errors = 0
Rx OutofRange Errors = 0
```

Example (Linecard: Drops)

```
Dell#show hardware linecard 2 drops

UNIT No: 0
Total Ingress Drops           : 3235
Total IngMac Drops            : 0
Total Mmu Drops               : 0
Total EgMac Drops             : 0
Total Egress Drops            : 0
```

Example (Linecard Unit: Drops)

```
Dell#show hardware linecard 2 drops unit 0

UserPort    PortNumber    Ingress Drops   IngMac Drops    Total Mmu Drops
EgMac Drops    Egress Drops
 0               1               0               0
0               0               0
 4               5               0               0
0               0               0
 8               9               0               0
0               0               0
 12              13              3258            0
0               0               0
 16              17              0               0
0               0               0
 17              18              0               0
0               0               0
 18              19              0               0
0               0               0
 19              20              0               0
0               0               0
 20              21              0               0
0               0               0
 21              22              0               0
0               0               0
 22              23              0               0
0               0               0
 23              24              0               0
0               0               0
 24              25              0               0
0               0               0
 28              29              0               0
0               0               0
 32              33              0               0
0               0               0
 36              37              0               0
0               0               0
 40              41              0               0
0               0               0
 44              45              0               0
0               0               0
 Internal        50              0               0
```

```
0               0               0
 Internal        51              0               0
0               0               0
 Internal        52              0               0
0               0               0
 Internal        53              0               0
0               0               0
 Internal        54              0               0
0               0               0
 Internal        55              0               0
0               0               0
 Internal        56              0               0
0               0               0
 Internal        57              0               0
0               0               0
 Internal        58              0               0
0               0               0
 Internal        59              0               0
0               0               0
 Internal        60              0               0
0               0               0
 Internal        61              0               0
0               0               0
```

Example (Linecard Unit Port: Drops)

```
Dell#show hardware linecard 2 drops unit 0 port 12

Drops in UserPort 12:
 --- Ingress Drops      ---
Ingress Drops                  : 3299
IBP CBP Full Drops             : 0
PortSTPnotFwd Drops            : 0
IPv4 L3 Discards               : 0
Policy Discards                : 0
Packets dropped by FP          : 3299
(L2+L3) Drops                  : 0
Port bitmap zero Drops         : 0
Rx VLAN Drops                  : 0
 --- Ingress MAC counters---
Ingress FCSDrops               : 0
Ingress MTUExceeds             : 0
 --- MMU Drops          ---
HOL DROPS(TOTAL)               : 0
HOL DROPS on COS0              : 0
HOL DROPS on COS1              : 0
HOL DROPS on COS2              : 0
HOL DROPS on COS3              : 0
HOL DROPS on COS4              : 0
HOL DROPS on COS5              : 0
HOL DROPS on COS6              : 0
HOL DROPS on COS7              : 0
HOL DROPS on COS8              : 0
HOL DROPS on COS9              : 0
HOL DROPS on COS10             : 0
HOL DROPS on COS11             : 0
HOL DROPS on COS12             : 0
HOL DROPS on COS13             : 0
HOL DROPS on COS14             : 0
HOL DROPS on COS15             : 0
HOL DROPS on COS16             : 0
HOL DROPS on COS17             : 0
HOL DROPS on COS18             : 0
HOL DROPS on COS19             : 0
HOL DROPS on COS20             : 0
TxPurge CellErr                : 0
Aged Drops                     : 0
 --- Egress MAC counters---
Egress FCS Drops               : 0
 --- Egress FORWARD PROCESSOR Drops   ---
```

```
IPv4 L3UC Aged & Drops        : 0
TTL Threshold Drops           : 0
INVALID VLAN CNTR Drops       : 0
L2MC Drops                    : 0
PKT Drops of ANY Conditions   : 0
Hg MacUnderflow               : 0
TX Err PKT Counter            : 0
 --- Error counters---
Internal Mac Transmit Errors  : 0
Unknown Opcodes               : 0
Internal Mac Receive Errors   : 0
```

Example (Linecard Unit: Port-Stats)

```
Dell#show hardware linecard 2 unit 0 port-stats
          ena/  speed/ link auto    STP                 lrn  inter   max
loop
     port link  duplex scan neg?   state   pause  discrd ops   face frame
back
       xe0  !ena  40G FD   SW  No   Forward           Tag    F    CR4  1550
       xe1  !ena  40G FD   SW  No   Forward           Tag    F  XGMII  1550
       xe2  !ena  40G FD   SW  No   Forward           Tag    F  XGMII  1550
       xe3  up    40G FD   SW  No   Forward           Tag    F    SR4  1550
       xe4  down  10G FD   SW  No   Forward           Tag    F    SFI  1550
       xe5  down  10G FD   SW  No   Forward           Tag    F    SFI  1550
       xe6  down  10G FD   SW  No   Forward           Tag    F    SFI  1550
       xe7  down  10G FD   SW  No   Forward           Tag    F    SFI  1550
       xe8  up    10G FD   SW  No   Forward           Tag    F    SFI  1550
       xe9  !ena  10G FD   SW  No   Forward           Tag    F    SFI  1550
      xe10  !ena  10G FD   SW  No   Forward           Tag    F    SFI  1550
      xe11  !ena  10G FD   SW  No   Forward           Tag    F    SFI  1550
      xe12  !ena  40G FD   SW  No   Forward           Tag    F  XGMII  1550
      xe13  !ena  40G FD   SW  No   Forward           Tag    F  XGMII  1550
      xe14  !ena  40G FD   SW  No   Forward           Tag    F  XGMII  1550
      xe15  !ena  40G FD   SW  No   Forward           Tag    F  XGMII  1550
      xe16  !ena  40G FD   SW  No   Forward           Tag    F  XGMII  1550
      xe17  !ena  40G FD   SW  No   Forward           Tag    F  XGMII  1550
       ge0  up     1G FD   SW  No   Forward          None   FA   GMII 16360
       hg0  up    42G FD   SW  No   Forward          None    F  XGMII 16360
       hg1  up    42G FD   SW  No   Forward          None    F  XGMII 16360
       hg2  up    42G FD   SW  No   Forward          None    F  XGMII 16360
       hg3  up    42G FD   SW  No   Forward          None    F  XGMII 16360
       hg4  up    42G FD   SW  No   Forward          None    F  XGMII 16360
       hg5  up    42G FD   SW  No   Forward          None    F  XGMII 16360
       hg6  up    42G FD   SW  No   Forward          None    F  XGMII 16360
       hg7  up    42G FD   SW  No   Forward          None    F  XGMII 16360
       hg8  up    42G FD   SW  No   Forward          None    F  XGMII 16360
       hg9  up    42G FD   SW  No   Forward          None    F  XGMII 16360
      hg10  up    42G FD   SW  No   Forward          None    F  XGMII 16360
      hg11  up    42G FD   SW  No   Forward          None    F  XGMII 16360
```

Example (Linecard Unit: Register)

```
Dell#show hardware linecard 2 unit 0 register
0x77120000 ARB_RAM_DBGCTRL.ipipe0 = 0x00000000
0x04000134 ASF_PORT_CFG.cpu0 = 0x00000000
0x04000107 ASF_PORT_CFG.xe0 = 0x0000001c
0x04000109 ASF_PORT_CFG.xe1 = 0x0000001c
0x0400010b ASF_PORT_CFG.xe2 = 0x0000001c
0x04000141 ASF_PORT_CFG.xe3 = 0x0000001c
0x0400014a ASF_PORT_CFG.xe4 = 0x0000000c
0x0400014b ASF_PORT_CFG.xe5 = 0x0000000c
0x0400014c ASF_PORT_CFG.xe6 = 0x0000000c
0x0400014d ASF_PORT_CFG.xe7 = 0x0000000c
0x0400014e ASF_PORT_CFG.xe8 = 0x0000000c
0x0400014f ASF_PORT_CFG.xe9 = 0x0000000c
0x04000150 ASF_PORT_CFG.xe10 = 0x0000000c
0x04000151 ASF_PORT_CFG.xe11 = 0x0000000c
0x04000106 ASF_PORT_CFG.xe12 = 0x0000001c
0x04000108 ASF_PORT_CFG.xe13 = 0x0000001c
0x0400010a ASF_PORT_CFG.xe14 = 0x0000001c
0x04000140 ASF_PORT_CFG.xe15 = 0x0000001c
```

```
0x04000142 ASF_PORT_CFG.xe16 = 0x0000001c
0x04000143 ASF_PORT_CFG.xe17 = 0x0000001c
0x0400010c ASF_PORT_CFG.ge0 = 0x00000007
0x04000144 ASF_PORT_CFG.hg0 = 0x0000001d
0x04000145 ASF_PORT_CFG.hg1 = 0x0000001d
0x04000147 ASF_PORT_CFG.hg2 = 0x0000001d
0x04000146 ASF_PORT_CFG.hg3 = 0x0000001d
0x04000149 ASF_PORT_CFG.hg4 = 0x0000001d
0x04000148 ASF_PORT_CFG.hg5 = 0x0000001d
0x04000100 ASF_PORT_CFG.hg6 = 0x0000001d
0x04000101 ASF_PORT_CFG.hg7 = 0x0000001d
0x04000103 ASF_PORT_CFG.hg8 = 0x0000001d
0x04000102 ASF_PORT_CFG.hg9 = 0x0000001d
0x04000105 ASF_PORT_CFG.hg10 = 0x0000001d
0x04000104 ASF_PORT_CFG.hg11 = 0x0000001d
0x04000174 ASF_PORT_CFG.lb0 = 0x00000000
0x77000000 AUX_ARB_CONTROL.ipipe0 = 0x00000012
0x77010000 AUX_ARB_CONTROL_2.ipipe0 = 0x64ff40a3
0x16004a00 BFD_RX_ACH_TYPE_CONTROL0.ipipe0 = 0x00570021
0x16004b00 BFD_RX_ACH_TYPE_CONTROL1.ipipe0 = 0x00000007
0x16004c00 BFD_RX_ACH_TYPE_MPLSTP.ipipe0 = 0x00000000
0x16005300 BFD_RX_ACH_TYPE_MPLSTP1.ipipe0 = 0x0000000000000000
0x0a009900 BFD_RX_UDP_CONTROL.ipipe0 = 0x0ec812b0
0x16004900 BFD_RX_UDP_CONTROL_1.ipipe0 = 0x0ec812b0
0x26001500 BKPMETERINGDISCSTATUS0.mmu0 = 0x0000000000000000
0x26001600 BKPMETERINGDISCSTATUS1.mmu0 = 0x0000000000000000
0x26001000 BKPMETERINGWARNSTATUS0.mmu0 = 0x0000000000000000
0x26001100 BKPMETERINGWARNSTATUS1.mmu0 = 0x0000000000000000
0x32000900 BST_HW_SNAPSHOT_EN.mmu0 = 0x00000000
0x32000800 BST_SNAPSHOT_ACTION_EN.mmu0 = 0x00000000
0x32000700 BST_TRACKING_ENABLE.mmu0 = 0x00000000
0x56002000 BUF_CFG(0).mmu0 = 0x00000000
0x56002001 BUF_CFG(1).mmu0 = 0x00000000
0x56002002 BUF_CFG(2).mmu0 = 0x00000000
0x56002003 BUF_CFG(3).mmu0 = 0x00000000
0x56002004 BUF_CFG(4).mmu0 = 0x00000000
0x56002005 BUF_CFG(5).mmu0 = 0x00000000
0x56002006 BUF_CFG(6).mmu0 = 0x00000000
0x56002007 BUF_CFG(7).mmu0 = 0x00000000
0x56002008 BUF_CFG(8).mmu0 = 0x00000000
0x56002009 BUF_CFG(9).mmu0 = 0x00000000
0x5600200a BUF_CFG(10).mmu0 = 0x00000000
0x5600200b BUF_CFG(11).mmu0 = 0x00000000
0x5600200c BUF_CFG(12).mmu0 = 0x00000000
0x5600200d BUF_CFG(13).mmu0 = 0x00000000
0x5600200e BUF_CFG(14).mmu0 = 0x00000000
0x5600200f BUF_CFG(15).mmu0 = 0x00000000
0x36000200 CBL_ATTRIBUTE(0).ipipe0 = 0x00000000
0x36000201 CBL_ATTRIBUTE(1).ipipe0 = 0x00000000
0x36000202 CBL_ATTRIBUTE(2).ipipe0 = 0x00000000
0x36000203 CBL_ATTRIBUTE(3).ipipe0 = 0x00000000
0x37040000 CCM_INTERRUPT_CONTROL.ipipe0 = 0x00000000
0x37030000 CCM_READ_CONTROL.ipipe0 = 0x00000000
0x22001200 CCPMEMDEBUG.mmu0 = 0x00000000
0x22001000 CCP_STS.mmu0 = 0x00000003
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl0 = 0x0000000000000010
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl1 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl2 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl3 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl4 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl5 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl6 = 0x0000000000000000
0x02001a00 CELL_ASM_0_CONTROL.pgw_cl7 = 0x0000000000000000
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_cl0 = 0x00000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_cl1 = 0x00000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_cl2 = 0x00000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_cl3 = 0x00000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_cl4 = 0x00000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_cl5 = 0x00000000000318c6
```

```
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_cl6 = 0x00000000000318c6
0x02004500 CELL_ASM_CUT_THRU_THRESHOLD.pgw_cl7 = 0x00000000000318c6
0x12002000 CELL_LINK_MEM_DEBUG_TM.mmu0 = 0x00000000
0x1e001000 CFAPBANKFULL(0).mmu0 = 0x000007ff
0x1e001001 CFAPBANKFULL(1).mmu0 = 0x000007ff
0x1e001002 CFAPBANKFULL(2).mmu0 = 0x000007ff
0x1e001003 CFAPBANKFULL(3).mmu0 = 0x000007ff
0x1e001004 CFAPBANKFULL(4).mmu0 = 0x000007ff
0x1e001005 CFAPBANKFULL(5).mmu0 = 0x000007ff
0x1e001006 CFAPBANKFULL(6).mmu0 = 0x000007ff
0x1e001007 CFAPBANKFULL(7).mmu0 = 0x000007ff
0x1e001008 CFAPBANKFULL(8).mmu0 = 0x000007ff
0x1e001009 CFAPBANKFULL(9).mmu0 = 0x000007ff
0x1e00100a CFAPBANKFULL(10).mmu0 = 0x000007ff
0x1e00100b CFAPBANKFULL(11).mmu0 = 0x000007ff
0x1e00100c CFAPBANKFULL(12).mmu0 = 0x000007ff
0x1e00100d CFAPBANKFULL(13).mmu0 = 0x000007ff
0x1e00100e CFAPBANKFULL(14).mmu0 = 0x000007ff
0x1e00100f CFAPBANKFULL(15).mmu0 = 0x000007ff
0x1e003000 CFAPBANKSTATUS(0).mmu0 = 0x00000028
0x1e003001 CFAPBANKSTATUS(1).mmu0 = 0x00000025
0x1e003002 CFAPBANKSTATUS(2).mmu0 = 0x00000022
0x1e003003 CFAPBANKSTATUS(3).mmu0 = 0x00000025
0x1e003004 CFAPBANKSTATUS(4).mmu0 = 0x00000023
0x1e003005 CFAPBANKSTATUS(5).mmu0 = 0x00000023
0x1e003006 CFAPBANKSTATUS(6).mmu0 = 0x00000027
0x1e003007 CFAPBANKSTATUS(7).mmu0 = 0x00000026
0x1e003008 CFAPBANKSTATUS(8).mmu0 = 0x00000027
!------------------ output truncated ---------------!
```

Example (Linecard Unit: Counters)

```
Dell#show hardware linecard  0 unit 1 counters
RUC.cpu0                  :               528,687            +528,687
ING_NIV_RX_FRAMES.cpu0    :               528,687            +528,687
TDBGC6.cpu0               :               528,687            +528,687
PERQ_PKT(0).cpu0          :                 1,172              +1,172
PERQ_PKT(41).cpu0         :               527,515            +527,515
PERQ_BYTE(0).cpu0         :                79,696             +79,696
PERQ_BYTE(41).cpu0        :            35,871,020         +35,871,020
PERQ_DROP_PKT(0).cpu0     :               217,930            +217,930
PERQ_DROP_PKT(41).cpu0    :         2,186,107,010      +2,186,107,010
PERQ_DROP_BYTE(0).cpu0    :            14,819,240         +14,819,240
PERQ_DROP_BYTE(41).cpu0   :       148,655,276,680    +148,655,276,680
QUEUE_PEAK(0).cpu0        :                   224
QUEUE_PEAK(41).cpu0       :                   236
RUC.xe0                   :         2,756,973,184      +2,756,973,184
RDBGC0.xe0                :         2,186,634,525      +2,186,634,525
RDBGC5.xe0                :         2,186,634,525      +2,186,634,525
ING_NIV_RX_FRAMES.xe0     :         2,756,973,184      +2,756,973,184
TDBGC3.xe0                :             2,881,121          +2,881,121
TDBGC6.xe0                :       190,692,963,094    +190,692,963,094
12,017,817/s
TDBGC10.xe0               :             2,881,121          +2,881,121
R127.xe0                  :         2,756,973,184      +2,756,973,184
RPKT.xe0                  :         2,756,973,184      +2,756,973,184
```

Example (Linecard Unit: Details)

```
Dell#show hardware linecard 2 unit 0 details

******************************************************

The total no of FP & CSF Devices in the Card is 1
The total no of FP Devices in the Card is 1
The total no of CSF Devices in the Card is 0
The number of ports in device 0 is - 18
The number of Hg ports in devices 0 is - 12
The CPU Port of the device is 0
The starting unit no the SWF in the device is 0
******************************************************
```

```
bcmLinkMonStatusShow: The Current Link Status Is

Front End Link Status        0x00080800 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000
Front End Port Presence      0x00000000 0x00000000 0x00000000 0x00000000
0x00000000 0x00000000
Backplane Link Status        0xc0000300 0x000c0000
*******************************************************

Link Status of all the ports in the Device - 0

The linkStatus of Front End Port 1 is FALSE
The linkStatus of Front End Port 5 is FALSE
The linkStatus of Front End Port 9 is FALSE
The linkStatus of Front End Port 13 is TRUE
The linkStatus of Front End Port 17 is FALSE
The linkStatus of Front End Port 18 is FALSE
The linkStatus of Front End Port 19 is FALSE
The linkStatus of Front End Port 20 is FALSE
The linkStatus of Front End Port 21 is TRUE
The linkStatus of Front End Port 22 is FALSE
The linkStatus of Front End Port 23 is FALSE
The linkStatus of Front End Port 24 is FALSE
The linkStatus of Front End Port 25 is FALSE
The linkStatus of Front End Port 29 is FALSE
The linkStatus of Front End Port 33 is FALSE
The linkStatus of Front End Port 37 is FALSE
The linkStatus of Front End Port 41 is FALSE
The linkStatus of Front End Port 45 is FALSE
The linkStatus of Hg Port 50 is TRUE
The linkStatus of Hg Port 51 is TRUE
The linkStatus of Hg Port 52 is TRUE
The linkStatus of Hg Port 53 is TRUE
The linkStatus of Hg Port 54 is TRUE
The linkStatus of Hg Port 55 is TRUE
The linkStatus of Hg Port 56 is TRUE
The linkStatus of Hg Port 57 is TRUE
The linkStatus of Hg Port 58 is TRUE
The linkStatus of Hg Port 59 is TRUE
The linkStatus of Hg Port 60 is TRUE
The linkStatus of Hg Port 61 is TRUE
*******************************************************

Trunk Info for Unit 0 ----------------------
The allocated Trunk ID is  - 1024
The PSC is                 - 9
The Current Trunk ID       - 1025
Init Done is               - 1
Trunk Valid is             - 1
Trunk Port Information
The flags is               - 0
The no of ports is         - 12
The PSC is                 - 9
The DLF Index is           - -1
The MC  Index is           - -1
The IPMC Index is          - -1
The tm-tp for Index 0 is    :  -1 | -1
The tm-tp for Index 1 is    :  -1 | -1
The tm-tp for Index 2 is    :  -1 | -1
The tm-tp for Index 3 is    :  -1 | -1
The tm-tp for Index 4 is    :  -1 | -1
The tm-tp for Index 5 is    :  -1 | -1
The tm-tp for Index 6 is    :  -1 | -1
The tm-tp for Index 7 is    :  -1 | -1
The tm-tp for Index 8 is    :  -1 | -1
The tm-tp for Index 9 is    :  -1 | -1
The tm-tp for Index 10 is    :  -1 | -1
The tm-tp for Index 11 is    :  -1 | -1
```

```
**********************************************

ModPort Table for Device - 0
For Destination Mod Id 0 Destination Port is 50
For Destination Mod Id 1 Destination Port is 50
For Destination Mod Id 2 Destination Port is 50
For Destination Mod Id 3 Destination Port is 50
For Destination Mod Id 4 Destination Port is 50
For Destination Mod Id 5 Destination Port is 50
For Destination Mod Id 6 Destination Port is 50
For Destination Mod Id 7 Destination Port is 50
For Destination Mod Id 9 Destination Port is 50
For Destination Mod Id 10 Destination Port is 50
For Destination Mod Id 11 Destination Port is 50
!------------------ output truncated ---------------!
```

Example (Linecard: Total-Buffer)

```
Dell(conf)#show hardware linecard 2 buffer total-buffer
------ Buffer Details for linecard 2 ------
Total Buffers allocated per linecard 61440
```

Example (Linecard Unit Port: Buffer-Info)

```
Dell(conf)#show hardware linecard 2 buffer unit 0 port 12 buffer-info
-----  Buffer Stats for Unit 0 Port 13 -----
 Maximum Shared Limit for the Port: 44537
 Default Packet Buffer allocate for the Port: 150
 Used Packet Buffer for the Port: 0
```

```
Dell(conf)#show hardware linecard 0 buffer unit 0 port 1 queue 1 buffer-info
-----  Buffer Stats for Unit 0 Port 1 Queue 1 -----
 Maximum Shared Limit: 27371
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
```

Example (Linecard: Backplane Links)

```
Dell#show hardware linecard 0 bp-link-map

 Back Plane HG Links
 ___________________________________________

LinkId          0       1       2       3       4       5       22      23
NpuId/PortId    0/56    0/57    1/56    1/57    2/56    2/57    0/58    0/59


LinkId          24      25      26      27      44      45      46      47
NpuId/PortId    1/58    1/59    2/58    2/59    0/60    0/61    1/60    1/61


LinkId          48      49      66      67      68      69      70      71
NpuId/PortId    2/60    2/61    0/50    0/51    1/50    1/51    2/50    2/51


LinkId          88      89      90      91      92      93      110     111
NpuId/PortId    0/52    0/53    1/52    1/53    2/52    2/53    0/54    0/55


LinkId          112     113     114     115
NpuId/PortId    1/54    1/55    2/54    2/55


Back Plane GE Links
_____________________________________

LinkId          138     139     140
NpuId/PortId    0/49    1/49    2/49
```

Example (Linecard: Backplane-link Status)

```
Dell#show hardware linecard 0 bp-link-state

 Total valid Links  - 39

Valid Link bmp             - 0xfc0003f0-000fc000-3f0000fc-0003f000-00380000

Valid Link bmp State       - 0xf40003f0-000fc000-3d0000fc-0003f000-00380000
```

Example (Linecard Unit Port: HiGig Port Statistics)

```
Dell#show hardware linecard 0 hg-stats unit 1 port 50
Higig Port Statistics:
HiGigabitEthernet 0/1/50,
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes 0 underruns
     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 Multicasts, 0 Broadcasts 0 Unicasts
     0 throttles, 0 discarded, 5208131494077267968 collisions
19141612676317184 wredDrops
Rate info (interval 15 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
```

Example (Port Extender Statistics)

```
Dell>show hardware pe 0 stack-unit 0 cpu data-plane statistics

bc pci driver statistics for device:
 rxHandle        :15451
 noMhdr          :0
 noMbuf          :0
 noClus          :0
 recvd           :15451
 dropped         :0
 recvToNet       :15451
 rxError         :0
 rxFwdError      :0
 rxDatapathErr   :0
 rxPkt(COS0 )    :0
 rxPkt(COS1 )    :0
 rxPkt(COS2 )    :0
 rxPkt(COS3 )    :0
 rxPkt(COS4 )    :0
 rxPkt(COS5 )    :0
 rxPkt(COS6 )    :9304
 rxPkt(COS7 )    :3
 rxPkt(COS8 )    :6144
 rxPkt(COS9 )    :0
 rxPkt(COS10)   :0
 rxPkt(COS11)   :0
 rxPkt(UNIT0)    :15451
 transmitted     :15250
 txRequested     :15250
 noTxDesc        :0
 txError         :0
 txReqTooLarge   :0
 txInternalError :0
 txDatapathErr   :0
 txPkt(COS0 )    :0
 txPkt(COS1 )    :0
 txPkt(COS2 )    :0
 txPkt(COS3 )    :0
 txPkt(COS4 )    :0
```

```
 txPkt(COS5 )     :0
 txPkt(COS6 )     :0
 txPkt(COS7 )     :0
 txPkt(COS8 )     :0
 txPkt(COS9 )     :0
 txPkt(COS10)    :0
 txPkt(COS11)    :0
 txPkt(UNIT0)     :0

Dell>show hardware pe 0 stack-unit 0 drops user-port 1
Dell#sho hardware pe 255 stack-unit 3 drops user-port 47
Drops in Interface PeGi 255/3/47:
--- Ingress Drops      ---
Ingress Drops                 : 13049
IBP CBP Full Drops            : 0
PortSTPnotFwd Drops           : 13049
IPv4 L3 Discards              : 0
Policy Discards               : 0
Packets dropped by FP         : 0
(L2+L3) Drops                 : 0
Port bitmap zero Drops        : 13049
Rx VLAN Drops                 : 0
--- Ingress MAC counters---
Ingress FCSDrops              : 0
Ingress MTUExceeds            : 0
--- MMU Drops          ---
Ingress MMU Drops             : 0
HOL DROPS(TOTAL)              : 1208454
HOL DROPS on COS0             : 0
HOL DROPS on COS1             : 0
HOL DROPS on COS2             : 0
HOL DROPS on COS3             : 0
HOL DROPS on COS4             : 0
HOL DROPS on COS5             : 0
```

Example (Forwarding-table mode)

```
Dell>show hardware forwarding-table mode

                    Current Settings
Mode              :  Default
L2 MAC Entries    :  160K
L3 Host Entries   :  144K
L3 Route Entries  :   16K
```

Related Commands

clear hardware system-flow — clears the statistics from selected hardware components.

show system — displays the current status of all the stack members or a specific member.

show hardware buffer

Display buffer statistics for a specified interface.

C9000 Series

Syntax

```
show hardware {interface interface [buffer-info | priority-group [group number
| all] | queue [queue number | all]]
```

Parameters

interface *interface*	Enter the keyword `interface` then type one of the following interface types and slot/port or number information: • For a 1–Gigabit Ethernet interface, enter the keyword `gigabitethernet`. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`. • For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigabitEthernet` then the *pe-id*, stack-unit *unit number*, and *port-id*. The *pe-id* range is 0–255; the stack unit number range is 0–7; and the port-ID range is 0 –47. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE. **NOTE: The peGigE or peTenGigE interface option is only available when the extended bridge is enabled.**
buffer-info	Enter the keyword `buffer-info` to view the total buffer allocated for the Interface
priority-group *group number | all*	Enter the keyword `priority-group` and specify a priority *group number* or *all* the priority groups. The range for priority group is from 0 to 7.
queue *queue number | all*	Enter the keyword `queue` and specify a *queue number* or select *all* for all the queues. The range for queue number is from 0 to 19.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.

Example (show hardware buffer interface peGige buffer-info)

```
Dell#show hardware buffer interface peGigE 10/1/1 buffer-info
-----  Buffer Stats for Interface  PeGi 10/1/1 -----
 Maximum Shared Limit for the Interface: 6956
 Default Packet Buffer allocate for the Interface: 160
 Used Packet Buffer for the Interface: 0
```

Example (priority-group 0)

```
Dell# show hardware buffer interface peGigE 10/1/1 priority-group 0 buffer-info
----- Buffer stats for unit: 0 port: 1 (interface PeGi 10/1/1) -----
-------------------------------------------------------------------------
PG# PRIORITIES             ALLOTED (CELLS)          COUNTER (CELLS)
                  MIN    SHARED    MODE    HDRM   MIN    SHARED  HDRM
-------------------------------------------------------------------------
0   -             19584  0         STATIC  174    0      0       0
```

Example (queue all)

```
Dell#show hardware buffer interface peGigE 10/1/1 queue all buffer-info
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 0 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 1 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 2 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 3 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 4 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 5 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 6 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 7 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 8 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 9 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 10 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 11 -----
 Maximum Shared Limit: 4637
 Default Packet Buffer allocate for the Queue: 8
 Used Packet Buffer: 0
-----  Buffer Stats for Interface PeGi 10/1/1 Queue 12 ----
```

Related Commands

clear hardware system-flow — clears the statistics from selected hardware components.

show system — displays the current status of all the stack members or a specific member.

show hardware ip

Display Layer 3 ACL or QoS data for a line card and port pipe.

C9000 Series

Syntax

```
show hardware ip {eg-acl | in-acl | qos} linecard slot-id | pe pe-id stack-unit
unit-number port-set port-pipe
```

Parameters

eg-acl	Enter the keyword `eg-acl` to display Layer 3 egress acl data.
in-acl	Enter the keyword `in-acl` to display Layer 3 ingress acl data.
qos	Enter the keyword `qos` to display QoS data.
linecard*slot-id*	Enter the `linecard slot-id` parameters to specify a line card. The range of slot IDs is from 0 to 11.
pe *pe-id*	Enter the keyword `pe` and the port extender ID. The range is from 0 to 255. **NOTE: The pe option is only visible when the feature extended bridge feature is enabled.**
stack-unit *unit-number*	Enter the keyword `stack-unit` and the stack unit number. The range is from 0 to 7.
port-set *port-pipe*	Enter the keywords `port-set port-pipe` parameters to specify a port pipe (set of ports) on a line card. The range of port-pipe numbers is 0.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Example

```
Dell#show hardware ip eg-acl linecard 0 port-set 0
EID 0x000011b9: gid=0xf,
         slice=2, slice_idx=0, part =0 prio=0x11b9, flags=0x10202, Installed,
Enabled
              tcam: color_indep=0,
 StageEgress
```

```
 Color
    Offset: 5 Width: 2
    DATA=0x00000001
    MASK=0x00000003
         action={act=RpDrop, param0=0(0), param1=0(0), param2=0(0),
param3=0(0)}
         policer=
         statistics={stat id 64  slice = 2 idx=1 entries=1}{Packets}

EID 0x000011b8: gid=0xf,
         slice=2, slice_idx=0x1, part =0 prio=0x11b8, flags=0x10202,
Installed, Enabled
              tcam: color_indep=0,
 StageEgress
 IpType
    Offset: 192 Width: 4
    DATA=0x00000000
    MASK=0x0000000e
L3Routable
    Offset: 156 Width: 1
    DATA=0x00000001
    MASK=0x00000001
 OutPort
    Offset: 185 Width: 7
    DATA=0x00000005
    MASK=0x0000007f
         action={act=DropCancel, param0=0(0), param1=0(0), param2=0(0),
param3=0(0)}
         policer=
         statistics={stat id 110  slice = 2 idx=4 entries=1}{Packets}

EID 0x00001101: gid=0xf,
         slice=2, slice_idx=0x2, part =0 prio=0x1101, flags=0x10202,
Installed, Enabled
              tcam: color_indep=0,
 StageEgress
 IpFrag
    Offset: 7 Width: 2
    DATA=0x00000000
    MASK=0x00000001
 IpType
Offset: 192 Width: 4
    DATA=0x00000000
    MASK=0x0000000e
 L3Routable
    Offset: 156 Width: 1
    DATA=0x00000001
    MASK=0x00000001
 OutPort
    Offset: 185 Width: 7
    DATA=0x00000005
    MASK=0x0000007f
         action={act=Drop, param0=0(0), param1=0(0), param2=0(0), param3=0(0)}
         policer=
         statistics={stat id 111  slice = 2 idx=4 entries=1}{Packets}
```

Example

```
Dell#show hardware ip in-acl pe 1 stack-unit 0 port-set 0

EID 0x00000fff: gid=0x1,
         slice=0, slice_idx=0, part =0 prio=0xfff, flags=0x10602, Installed,
Enabled
              tcam: color_indep=1024,
 IpType
    Offset: 325 Width: 4
    DATA=0x00000000
    MASK=0x0000000e
 InPort
    DATA=0x0000000000000000000000000000000000000000000000000000000000000004
```

```
    MASK=0x0000000000000000000000000000000000000000000000000fdfffffffffff
 InPorts
    DATA=0x0000000000000000000000000000000000000000000000000000000000000004
    MASK=0x0000000000000000000000000000000000000000000000000fdfffffffffff
 HiGig
    Offset: 320 Width: 1
    DATA=0x00000000
    MASK=0x00000001
 Stage
 SrcIp
    Offset: 153 Width: 32
    DATA=0x02020201
    MASK=0xffffffff
         action={act=CopyToCpuCancel, param0=0(0), param1=0(0), param2=0(0),
param3=0(0)}
         action={act=EtagNew, param0=327687(0x50007), param1=0(0),
param2=0(0), param3=0(0)}
         policer=
         statistics={stat id 166  slice = 5 idx=0 entries=1}{Packets}

EID 0x00000e01: gid=0x2,
         slice=1, slice_idx=0, part =0 prio=0xe01, flags=0x10602, Installed,
Enabled
              tcam: color_indep=1024,
 IpType
    Offset: 325 Width: 4
    DATA=0x00000000
    MASK=0x0000000e
 InPort
    DATA=0x0000000000000000000000000000000000000000000000000000000000000004
    MASK=0x0000000000000000000000000000000000000000000000000fdfffffffffff
 InPorts
    DATA=0x0000000000000000000000000000000000000000000000000000000000000004
    MASK=0x0000000000000000000000000000000000000000000000000fdfffffffffff
 HiGig
    Offset: 320 Width: 1
    DATA=0x00000000
    MASK=0x00000001
 Stage
 IpFrag
    Offset: 71 Width: 2
    DATA=0x00000001
    MASK=0x00000001
         action={act=CopyToCpuCancel, param0=0(0), param1=0(0), param2=0(0),
param3=0(0)}
         action={act=EtagNew, param0=327687(0x50007), param1=0(0),
param2=0(0), param3=0(0)}
         policer=
         statistics={stat id 167  slice = 6 idx=0 entries=1}{Packets}
```

show hardware ipv6

Display information about IPv6 ACLs used on a line card and port pipe.

C9000 Series

Syntax `show hardware ipv6 {eg-acl | in-acl} linecard` *slot-id* `port-set` *port-pipe*

Parameters

eg-acl | in-acl Enter either the keyword `eg-acl` or the keyword `in-acl` to display ingress or egress ACL data.

linecards*slot-id*	Enter the `linecard slot-id` parameters to specify a line card on the switch. The range of slot IDs is from 0 to 2.
port-set *port-pipe*	Enter the keywords `port-set port-pipe` parameters to specify a port pipe (set of ports) on a line card. The range of port-pipe numbers is: 0 to 2 on line card 0 and 0 to 3 on line cards 1 and 2.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Example

```
Dell#show hardware ipv6 eg-acl linecard 0 port-set 0
EID 0x000013ce: gid=0xd,
         slice=0, slice_idx=0, part =0 prio=0x13ce, flags=0x10202, Installed,
Enabled
              tcam: color_indep=0,
 StageEgress
         slice=1, slice_idx=0, part =1 prio=0x13ce, flags=0x10204, Installed,
Enabled
              tcam: color_indep=0,
    Offset: 1 Width: 8
    DATA=0x0000003a
    MASK=0x000000ff
 IpType
    Offset: 208 Width: 5
    DATA=0x00000004
    MASK=0x0000000c
 L3Routable
    Offset: 166 Width: 1
    DATA=0x00000001
    MASK=0x00000001
 OutPort
    Offset: 195 Width: 7
    DATA=0x00000001
    MASK=0x0000007f
         action={act=Drop, param0=0(0), param1=0(0), param2=0(0), param3=0(0)}
         policer=
         statistics=NULL

EID 0x0000130d: gid=0xd,
         slice=0, slice_idx=0x1, part =0 prio=0x130d, flags=0x10202,
Installed, Enabled
              tcam: color_indep=0,
 StageEgress
         slice=1, slice_idx=0x1, part =1 prio=0x130d, flags=0x10204,
Installed, Enabled
              tcam: color_indep=0,
```

```
IpType
   Offset: 208 Width: 5
   DATA=0x00000004
   MASK=0x0000000c
L3Routable
   Offset: 166 Width: 1
   DATA=0x00000001
   MASK=0x00000001
OutPort
   Offset: 195 Width: 7
   DATA=0x00000001
   MASK=0x0000007f
        action={act=Drop, param0=0(0), param1=0(0), param2=0(0), param3=0(0)}
        policer=
        statistics={stat id 110  slice = 0 idx=4 entries=1}{Packets}
```

Usage Information The port-set values are internal port numbers.

show hardware mac

Display information about the MAC ACLs used on a line card and port-sets.

C9000 Series

Syntax

```
show hardware mac {eg-acl {pe pe-id stack-unit unit-number port-set port-pipe-id counters | linecard slot-id port-set number}| in-acl {pe pe-id stack-unit unit-number port-set port-pipe-id counters | linecard slot-id port-set number }}
```

Parameters

eg-acl | in-acl	Enter either the keyword `eg-acl` or the keyword `in-acl` to display ingress or egress ACL data.
linecards*slot-id*	Enter the `linecard slot-id` parameters to specify a line card. The range of slot IDs is from 0 to 11.
pe *pe-id*	Enter the `pepe-id` parameters to specify a port extender (PE). The PE ID range is from 0 to 255. **NOTE: The pe option is only visible when the extended bridge feature is enabled.**
stack-unit *unit-number*	Enter the `stack-unitunit-number` parameters to specify a stack-unit. The stack-unit range is from 0 to 7.
port-set *number*	Enter the keyword `port-set number` parameters to specify a port pipe (set of ports) on a line card. The port set number is 0.
counters	Enter the keyword `counters` to display counter statistics.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Usage Information The port-set values are internal port numbers.For more information on the interfaces and port numbers, see the *Debugging and Diagnostics* chapter in the *Dell Networking OS Configuration Guide for the C9000 System*.

Example

```
Dell#show hardware mac in-acl pe 8 stack-unit 0 port-set 0
EID 0x00000c00: gid=0x5,
slice=6, slice_idx=0, part =0 prio=0xc00, flags=0x10602, Installed, Enabled
tcam: color_indep=1024,
Stage
InPort
DATA=0x00000000000000000000000000000000000000000000000001000000000
MASK=0x00000000000000000000000000000000000000000000000fdfffffffffff
InPorts
DATA=0x00000000000000000000000000000000000000000000000001000000000
MASK=0x00000000000000000000000000000000000000000000000fdfffffffffff
HiGig
Offset: 320 Width: 1
DATA=0x00000000
MASK=0x00000001
SrcMac
Offset: 89 Width: 48
DATA=0x00000000 08000000
MASK=0x0000ffff ffffffff
action={act=CopyToCpuCancel, param0=0(0), param1=0(0), param2=0(0),
param3=0(0)}
action={act=EtagNew, param0=65772(0x100ec), param1=0(0), param2=0(0),
param3=0(0)}
policer=
statistics=NULL

EID 0x00000bff: gid=0x5,
slice=6, slice_idx=0x1, part =0 prio=0xbff, flags=0x10202, Installed, Enabled
tcam: color_indep=0,
Stage
InPort
DATA=0x00000000000000000000000000000000000000000000000001000000000
MASK=0x00000000000000000000000000000000000000000000000fdfffffffffff
InPorts
DATA=0x00000000000000000000000000000000000000000000000001000000000
MASK=0x00000000000000000000000000000000000000000000000fdfffffffffff
HiGig
Offset: 320 Width: 1
DATA=0x00000000
MASK=0x00000001
SrcMac
Offset: 89 Width: 48
DATA=0x00000000 08000100
MASK=0x0000ffff ffffffff
action={act=DropCancel, param0=0(0), param1=0(0), param2=0(0), param3=0(0)}
policer=
statistics=NULL
```

show hardware system-flow

This command displays hardware system-flow information.

C9000 Series

Syntax

```
show hardware system-flow {cp-switch | linecard slot-id port-set port number |
pe pe-id stack-unit unit-number port-set port-pipe-id } counters
```

Parameters

cp-switch	Enter the keyword `cp-switch` to display the counters for control traffic on the control plane.
linecard *slot-id*	Enter the `linecard slot-id` parameters to identify the line card on which you want to clear system-flow statistics. The range of slot IDs is from 0 to 11.
pe *peid*	Enter the keyword `pe` and the port extender (PE) ID to display the counters for a specified PE. The PE ID ranges is from 0 to 255. **NOTE: The pe option is only visible when the extended bridge feature is enabled.**
stack-unit *unit-number*	Enter the keyword `stack-unit` and unit number to display the counters for the specified stack-unit. The stack unit range is from 0 to 7.
port set *port-pipe*	Enter the keyword `port-set` and port-pipe number. The port-set number is 0.

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Example

```
Dell# show hardware system-flow pe 1 stack-unit 0 port-set  0
######### FP Entry for IPC traffic destined to stack_unit 4 PE CPU#######
EID 0x000003fb: gid=0xd,
     slice=11, slice_idx=0x5, part =0 prio=0x3fb,flags=0x10602,Installed,
Enabled
             tcam: color_indep=1024,
Stage
InPorts
    DATA=0x0000000000000000000000000000000000000000000000c000000000000
    MASK=0x0000000000000000000000000000000000000000000000ddddddddddddd
```

```
HiGig
   Offset: 320 Width: 1
   DATA=0x00000000
   MASK=0x00000001
DstIp
   Offset: 105 Width: 32
   DATA=0x7f080141
   MASK=0xffffffff
OuterVlanId
   Offset: 8 Width: 12
   DATA=0x00000ffc
   MASK=0x00000fff
     action={act=CosQNew, param0=8(0x8), param1=0(0), param2=0(0), param3=0(0)}
     action={act=RedirectPort, param0=4(0x4), param1=0(0), param2=0(0),
param3=0(0)}
     policer=
     statistics={stat id 58  slice = 0 idx=15 entries=1}{Packets}

######### FP Entry for IPC traffic destined to stack_unit 5 PE CPU#######
EID 0x000003fa: gid=0xd,
    slice=11, slice_idx=0x6, part =0 prio=0x3fa, flags=0x10602, Installed,
Enabled
     tcam: color_indep=1024,
 Stage
 InPorts
    DATA=0x0000000000000000000000000000000000000000000000c000000000000
    MASK=0x0000000000000000000000000000000000000000000000ddddddddddddd
 HiGig
    Offset: 320 Width: 1
    DATA=0x00000000
    MASK=0x00000001
 DstIp
    Offset: 105 Width: 32
    DATA=0x7f080151
    MASK=0xffffffff
 OuterVlanId
    Offset: 8 Width: 12
    DATA=0x00000ffc
    MASK=0x00000fff
      action={act=CosQNew, param0=8(0x8), param1=0(0), param2=0(0),
param3=0(0)}
      action={act=RedirectPort, param0=5(0x5), param1=0(0), param2=0(0),
param3=0(0)}
      policer=
      statistics={stat id 59  slice = 0 idx=16 entries=1}{Packets}

######### FP Entry for IPC traffic destined to stack_unit 6 PE CPU#######
EID 0x000003f9: gid=0xd,
      slice=11, slice_idx=0x7, part =0 prio=0x3f9, flags=0x10602, Installed,
Enabled
           tcam: color_indep=1024,
 Stage
 InPorts
    DATA=0x0000000000000000000000000000000000000000000000c000000000000
    MASK=0x0000000000000000000000000000000000000000000000ddddddddddddd
 HiGig
    Offset: 320 Width: 1
    DATA=0x00000000
    MASK=0x00000001
 DstIp
    Offset: 105 Width: 32
    DATA=0x7f080161
    MASK=0xffffffff
 OuterVlanId
    Offset: 8 Width: 12
    DATA=0x00000ffc
    MASK=0x00000fff
       action={act=CosQNew, param0=8(0x8), param1=0(0), param2=0(0),
param3=0(0)}
```

```
       action={act=RedirectPort, param0=6(0x6), param1=0(0), param2=0(0),
param3=0(0)}
       policer=
       statistics={stat id 60  slice = 0 idx=17 entries=1}{Packets}

######### FP Entry for IPC traffic destined to stack_unit 7 PE CPU#######
EID 0x000003f8: gid=0xd,
     slice=11, slice_idx=0x8, part =0 prio=0x3f8, flags=0x10602, Installed,
Enabled
           tcam: color_indep=1024,
 Stage
 InPorts
    DATA=0x0000000000000000000000000000000000000000000c000000000000
    MASK=0x0000000000000000000000000000000000000000000dffffffffffff
 HiGig
   Offset: 320 Width: 1
   DATA=0x00000000
   MASK=0x00000001
 DstIp
   Offset: 105 Width: 32
   DATA=0x7f080171
   MASK=0xffffffff
 OuterVlanId
   Offset: 8 Width: 12
   DATA=0x00000ffc
   MASK=0x00000fff
      action={act=CosQNew, param0=8(0x8), param1=0(0), param2=0(0),
param3=0(0)}
      action={act=RedirectPort, param0=7(0x7), param1=0(0), param2=0(0),
param3=0(0)}
      policer=
      statistics={stat id 61  slice = 0 idx=18 entries=1}{Packets}
```

tcpdump

Enable a TCP dump for CPU-bound traffic on the Control and Router Processors..

C9000 Series

Syntax

`tcpdump {cp | rp} [capture-duration` *`time`* `| filter` *`expression`* `| max-file-count` *`value`* `| packet-count` *`value`* `| snap-length` *`value`* `| write-to` *`path`*`]`

To disable the TCP dump, use the `no tcpdump` command.

Parameters

cp	Enter the keyword `cp` to perform a dump on traffic processed by the Control Processor CPU.
rp	Enter the keyword `rp` to perform a dump on traffic processed by the Route Processor CPU.
capture-duration	Enter the time for packet capturing. The timer begins as soon as the command is enabled. The range is 20 to 9000 seconds.
filter	Specify the packet that will be dumped. If no filter is entered, all packets are dumped. Filter expressions usually consist of an id (name or num ber) preceded by one or more qualifiers. There are three different kinds of qualifier: type, direction, or protocol. Enclose the filter option with double quotes: “port 20.” The range is 1 to 100 characters.

max-file-count	Enter the maximum number of 1MB files. The maximum file size for a TCP dump capture is 1MB. When a file reaches 1MB, a new file is created, up to the specified number. The range is 1 to 20.
packet-count	Enter the number of packets to capture. The counter begins as soon as the command is enabled. The range is 10 to 150000.
snap-length	Enter the number of bytes per packet to capture. Use this option to reduce the size of the captured packets, to capture only the needed headers and avoid rest of the data portion of the packet. The range is 0 to 1200.
write-to	Enter the location to save the captured packets. Files can be saved to flash, to FTP, SCP, or TFTP: · `flash://filepath` · `ftp://userid:password@hostip/filepath` · `scp://userid:password@hostip/filepath` · `tftp://hostip/filepath`

Defaults TCP dumps are disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information Use the `tcpdump` command to perform a packet capture on a specified switch CPU: Control Processor (CP) or Route Processor (RP).

You can use the capture-duration timer and the packet-count counter at the same time. The TCP dump stops when the first of the thresholds is met. That means that even if the duration timer is 9000 seconds, if the maximum file count parameter is met first, the dumps stop.

The files saved on the flash are located in the flash://TCP_DUMP_DIR/Tcpdump_<time_stamp_dir>/directory. The file name is tcpdump_*.pcap. There can be up to 20 Tcpdump_<time_stamp_dir> directories. If more than 20 files are created, the oldest is overwritten.

Entering the `no tcpdump` command stops any TCP dump process running in either the Control Processor or Route Processor. The dump stops immediately, without waiting for a threshold to be met.

To stop the TCP dump process running in the CP processor, enter the `no tcpdump cp` command; to stop the TCP dump process running in the RP processor, enter the `no tcpdump rp` command.

13

Dynamic Host Configuration Protocol (DHCP)

Dynamic host configuration protocol (DHCP) is an application layer protocol that dynamically assigns IP addresses and other configuration parameters to network end-stations (hosts) based on the configuration policies the network administrators determine.

The Dell Networking OS supports the basic DHCP commands as described in the following sections:

- Configure a DHCP Server and DHCP Clients
- Configure Secure DHCP and DHCP Relay

Topics:

- Configure a DHCP Server and DHCP Clients
- Configure Secure DHCP and DHCP Relay

Configure a DHCP Server and DHCP Clients

To configure the system to be a DHCP server and to manually configure DHCP clients, use the following commands.

clear ip dhcp

Reset the DHCP counters.

C9000 Series

Syntax

```
clear ip dhcp [binding {address} | client statistics {all | interface type slot/port}| conflict | server statistics]
```

Parameters

binding	Enter the keyword `binding` to delete all entries in the binding table.
address	Enter the IP address to clear the binding entry for a single IP address.
client statistics {all | interface *type slot/port*}	Enter the keywords `server statistics all` to clear all counter information on all DHCP client interfaces on the switch. Enter an interface type and slot/port information to clear DHCP counters on a specified interface. The valid interface types are: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.
conflicts	Enter the keyword `conflicts` to delete all of the log entries created for IP address conflicts.
server statistics	Enter the keywords `server statistics` to clear all counter information on the DHCP server.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820t.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Usage Information Entering <CR> after the `clear ip dhcp binding` command clears all the IPs from the binding table.

debug ip dhcp client events

Activate the debugging and display of log messages on DHCP client interfaces for IP address acquisition, IP address release, and IP address and lease time renewal.

C9000 Series

Syntax `debug ip dhcp client events [interface type slot/port]`

Parameters

interface *typeslot/port* Enter the keyword `interface` with the interface type and slot/port information to display DHCP event messages for a specified interface. The valid interface types are:

- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# debug ip dhcp client events

Dell(conf-if-fo-2/0)#do show debugging
Dhcp Client :
 DhcpClient Event debugging is on for fortyGigE 2/0

Dell(conf-if-fo-2/0)#ip address dhcp
Dell(conf-if-fo-2/0)#no ip address dhcp

Dell(conf-if-fo-2/0)#do show logging
Syslog logging: enabled
    Console logging: level debugging
    Monitor logging: level debugging
    Buffer logging: level debugging, 9 Messages Logged, Size (40960 bytes)
    Trap logging: level informational
        Logging to 10.10.10.4
        Logging to 10.1.2.4
        Logging to 172.31.1.4
        Logging to 133.33.33.4
        Logging to 172.16.1.162
    Last logging buffer cleared: Jan 7 01:38:04
Jan 7 01:38:42: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG: DHCLIENT_DBG_EVT:
Interface Fo 2/0 :DHCP DISABLED CMD sent to FTOS in state START
Jan 7 01:38:41: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG: DHCLIENT_DBG_EVT:
Interface Fo 2/0 :Transitioned to state START
Jan 7 01:38:41: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG: DHCLIENT_DBG_EVT:
Interface Fo 2/0 :DHCP DISABLE CMD Received in state BOUND
Jan 7 01:38:07: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG: DHCLIENT_DBG_EVT:
Interface Fo 2/0 :DHCP ENABLE CMD Received in state START

Message                 Sent
BOOTREPLY               0
DHCPOFFER               10
DHCPACK                 16
DHCPNAK                 0
```

debug ip dhcp client packets

Activate the debugging and display of log messages for DHCP packets sent and received on DHCP client interfaces.

C9000 Series

Syntax `debug ip dhcp client packets [interface type slot/port]`

Parameters

interface *typeslot/port*	Enter the keyword `interface` with the interface type and slot/port information to display DHCP log messages for a specified interface. The valid interface types are: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# debug ip dhcp client packets

Dell(conf)#do show debugging
Dhcp Client :
 DhcpClient Packet debugging is on for fortyGigE 2/0

Dell(conf-if-fo-2/0)#ip address dhcp
Dell(conf-if-fo-2/0)#no ip address dhcp

Dell(conf-if-fo-2/0)#do show logging
Syslog logging: enabled
    Console logging: level debugging
    Monitor logging: level debugging
    Buffer logging: level debugging, 5 Messages Logged, Size (40960 bytes)
    Trap logging: level informational
        Logging to 10.10.10.4
        Logging to 10.1.2.4
        Logging to 172.31.1.4
        Logging to 133.33.33.4
        Logging to 172.16.1.162
    Last logging buffer cleared: Jan 7 01:41:17
Jan 7 01:42:34: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG: DHCLIENT_DBG_PKT:  DHCP
RELEASE sent in Interface Fo 2/0
Jan 7 01:41:39: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG: DHCLIENT_DBG_PKT:
Received DHCPACK packet in InterfaceFo 2/0 with Lease-IP:100.1.1.253, Mask:
255.255.255.0, Server-Id:100.1.1.2
Jan 7 01:41:39: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG: DHCLIENT_DBG_PKT:  DHCP
REQUEST sent in Interface Fo 2/0
Jan 7 01:41:36: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG: DHCLIENT_DBG_PKT:
Received DHCPOFFER packet in Interface Fo 2/0 with Lease-Ip:100.1.1.253, Mask:
255.255.255.0,Server-Id:100.1.1.2
Jan 7 01:41:36: %SYSTEM:CP %DHCLIENT-5-DHCLIENT-LOG: DHCLIENT_DBG_PKT:  DHCP
DISCOVER sent in Interface Fo 2/0
```

debug ip dhcp server

Display Dell OS debugging messages for DHCP.

C9000 Series

Syntax `debug ip dhcp server [events | packets]`

Parameters

events	Enter the keyword `events` to display the DHCP state changes.
packet	Enter the keyword `packet` to display packet transmission/reception.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

default-router

Assign a default gateway to clients based on the address pool.

C9000 Series

Syntax `default-router address [address2...address8]`

Parameters

address	Enter a list of routers that may be the default gateway for clients on the subnet. You may specify up to eight routers. List them in order of preference.

Defaults none

Command Modes DHCP <POOL>

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

disable

Disable the DHCP server.

C9000 Series

Syntax `disable`

DHCP Server is disabled by default. To enable the system to be a DHCP server, use the `no disable` command.

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

dns-server

Assign a DNS server to clients based on address pool.

C9000 Series

Syntax `dns-server address [address2...address8]`

Parameters

address	Enter a list of DNS servers that may service clients on the subnet. You may list up to eight servers, in order of preference.

Defaults none

Command Modes DHCP <POOL>

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

domain-name

Assign a domain to clients based on the address pool.

C9000 Series

Syntax `domain-name name`

Parameters

name	Give a name to the group of addresses in a pool.

Defaults none

Command Modes DHCP <POOL>

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

excluded-address

Prevent the server from leasing an address or range of addresses in the pool.

C9000 Series

Syntax `excluded-address [address | low-address high-address]`

Parameters

address	Enter a single address to be excluded from the pool.
low-address	Enter the lowest address in a range of addresses to be excluded from the pool.
high-address	Enter the highest address in a range of addresses to be excluded from the pool.

Defaults none

Command Modes DHCP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

hardware-address

For manual configurations, specify the client hardware address.

C9000 Series

Syntax `hardware-address address`

Parameters

address	Enter the hardware address of the client.

Defaults none

Command Modes DHCP <POOL>

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

host-address

For manual (rather than automatic) configurations, assign a host to a single-address pool.

Syntax `host–address address`

Parameters

address	Enter the host IP address.

Defaults None

Command Modes DHCP-POOL

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14.1.3	This command replaces `host` command. Introduced on S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, S6000, S4810, S4820T, S5048F-ON, MXL, FN-IOM, and C9010.

Usage Information When you upgrade the Dell EMC Networking OS from an earlier version to 9.14.1.3 or later, the system converts the DHCP CONFIGURATION `host` command in the running configuration to the `host-address` command. If you downgrade the Dell EMC Networking OS from version 9.14.1.3 or later to an earlier version, any existing `host-address` command is deleted from the running configuration. If you want to create manual DHCP bindings, use the `host` command.

ip address dhcp

Configure an interface to receive its IP address from the configured DHCP server.

C9000 Series

Syntax `ip address dhcp`

To release the IP address acquired from a DHCP server, enter the `no ip address dhcp` command.

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

You must be in INTERFACE mode in order to configure an interface to dynamically acquire an IP address from a DHCP server.

Use the `no ip address dhcp` in INTERFACE mode to:

- Release the IP address that was dynamically acquired from a DHCP server from the interface.
- Disable the DHCP client on the interface so it cannot acquire a dynamic IP address from a DHCP server.
- Stop DHCP packet transactions on the interface.

To release the IP address dynamically acquired from a DHCP server and allow an interface to acquire a new DHCP server-assigned address, enter the `release dhcp interface` *`type slot/port`* command in EXEC Privilege mode. To acquire a new server-assigned IP address, enter the `renew dhcp interface` *`type slot/port`* command in EXEC Privilege mode or the `ip address dhcp` command in INTERFACE Configuration mode.

ip address dhcp relay information-option

Include the relay-information option (option 82) in DHCP packets sent by the client. Some DHCP servers can be configured to allocate IP addresses based on option 82.

C9000 Series

Syntax

`ip address dhcp relay information-option [remote-id [`*`hostname`* | `mac` | *`remote-id`*`]`

Parameters

remote-id *hostname*	Set the hostname as the remote ID in Option 82.
remote-id *remote-id*	Enter the name to be used as the remote ID in Option 82; maximum: 64 characters.
remote-id mac	Use the chassis MAC address as the remote ID in Option 82.

Default

Option 82 uses the chassis MAC address as the remote ID.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Usage Information You can enter the `ip address dhcp relay information` and the `vendor-class indentifier`, for example:

```
ip address dhcp relay information-option remote-id mac

ip address dhcp relay information-option remote-id mac vendor-class-identifier
```

Related Commands ip address dhcp — configures an interface to receive its IP address from the configured DHCP server.

ip address dhcp vendor-class-identifier

Include the vendor-class identifier option (option 60) in DHCP packets sent by the client.

C9000 Series

Syntax

```
ip address dhcp vendor-class-identifier text
```

Parameters

vendor-class-identifier *text*	Include a user-configurable text string with the hardware-related information (option 60) in DHCP packets sent by the client (32 characters maximum).

Default None.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Usage Information Use this command to include the vendor-class identifier (option 60) in DHCP packets sent by the client. This option is used by DHCP clients to identify the vendor type and configuration of a DHCP client. The vendor-class identifier includes hardware-related information that identifies the switch and includes a user-configurable text string .

```
ip address dhcp vendor-class-identifier relay information-option

ip address dhcp vendor-class-identifier relay information-option remote-id mac
```

Related Commands ip address dhcp — configures an interface to receive its IP address from the configured DHCP server.

ip dhcp relay secondary-subnet

Enable DHCP relay secondary-subnet on all the interfaces in a switch.

C9000 Series

Syntax `[no] ip dhcp relay seconday-subnet`

To disable the dhcp relay secondary-subnet, use the`no ip dhcp relay secondary-subnet` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.

Example

```
Dell(conf)#ip dhcp relay secondary-subnet
```

ip dhcp server

Enable DHCP server globally.

Syntax `[no] ip dhcp server`

To disable the DHCP server, use the `no ip dhcp server` command.

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.12(1.0)	Introduced on the S5048F–ON.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.

Version	Description
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the S4810 and S4820T.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

ip helper-address

Specify the address of a DHCP server so that DHCP broadcast messages are forwarded when the DHCP server is not on the same subnet as the client.

C9000 Series

Syntax

`ip helper-address` *`ip-address`*

To remove a DHCP server address, use the `no ip helper-address` command.

Parameters

ip-address	Enter an IP address in dotted decimal format (A.B.C.D).

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Added support for IPv6.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

You can add multiple DHCP servers by entering the `ip helper-address` command multiple times. If multiple servers are defined, an incoming request is sent simultaneously to all configured servers and the reply is forwarded to the DHCP client.

The system uses standard DHCP ports, that is UDP ports 67 (server) and 68 (client) for DHCP relay services. It listens on port 67 and if it receives a broadcast, the software converts it to unicast, and forwards to it to the DHCP-server with source port=68 and destination port=67.

The server replies with source port=67, destination port=67 and the system forwards to the client with source port=67, destination port=68.

ipv6 helper-address

Configures the IPv6 DHCP helper addresses.

C9000 Series

Syntax

`[no] ipv6 helper-address [vrf vrf-name] ipv6-address`

To delete the ipv6 helper address, use the `[no] ipv6 helper-address [vrf vrf-name] ipv6-address` command.

Parameters

vrf *vrf-name*	(Optional) Enter the keyword `vrf` and then the name of the VRF through which the host address can be reached.
ipv6-address	Enter the keyword`ipv6-address` through which the server address can be reached.

Default Disabled.

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.14(1.0)	Enhanced to support non-default VRF configuration for DHCPv6 helper address.
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S4810, S4820T, S6000, S6000–ON, Z9000, and Z9500.

Usage Information Use this command on the interfaces where the DHCP clients are connected to forward the packets from clients to DHCP server and vice-versa.

Example

```
Dell(conf-if-te-0/0)#ipv6 helper-address
X:X:X:X::X     IPv6 helper address
VRF                                VRF name.
```

lease

Specify a lease time for the addresses in a pool.

C9000 Series

Syntax `lease {days [hours] [minutes] | infinite}`

Parameters

days	Enter the number of days of the lease. The range is from 0 to 31.
hours	Enter the number of hours of the lease. The range is from 0 to 23.
minutes	Enter the number of minutes of the lease. The range is from 0 to 59.
infinite	Specify that the lease never expires.

Defaults **24 hours**

Command Modes DHCP <POOL>

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Inroduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

netbios-name-server

Specify the NetBIOS Windows Internet Naming Service (WINS) name servers, in order of preference, that are available to Microsoft Dynamic Host Configuration Protocol (DHCP) clients.

C9000 Series

Syntax `netbios-name-server address [address2...address8]`

Parameters

address	Enter the address of the NETBIOS name server. You may enter up to eight, in order of preference.

Defaults none

Command Modes DHCP <POOL>

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

netbios-node-type

Specify the NetBIOS node type for a Microsoft DHCP client. Dell Networking recommends specifying clients as `hybrid`.

C9000 Series

Syntax `netbios-node-type type`

Parameters

type	Enter the NETBIOS node type: • Broadcast: Enter the keyword `b-node`. • Hybrid: Enter the keyword `h-node`. • Mixed: Enter the keyword `m-node`. • Peer-to-peer: Enter the keyword `p-node`.

Defaults **Hybrid**

Command Modes DHCP <POOL>

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

network

Specify the range of addresses in an address pool.

C9000 Series

Syntax `network network /prefix-length`

Parameters

network/ prefix-length	Specify a range of addresses. Prefix-length range is from 17 to 31.

Defaults none

Command Modes DHCP <POOL>

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

pool

Create an address pool.

C9000 Series

Syntax `pool name`

Parameters

name	Enter the address pool's identifying name.

Defaults none

Command Modes DHCP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

show ip dhcp client statistics

Display statistical information about DHCP client interfaces.

C9000 Series

Syntax `show ip dhcp client statistics [interface type slot/port]`

Parameters

interface *typeslot/port*	Enter the keyword `interface` with the interface type and slot/port information to display DHCP client information for a specified interface. The valid interface types are: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# show ip dhcp client statistics interface fortyGigE 2/0
Interface Name              Fo 2/0
Message                     Received
DHCPOFFER                   9
DHCPACK                     9
DHCPNAK                     0
Message                     Sent
DHCPDISCOVER                53
DHCPREQUEST                 9
DHCPDECLINE                 0
DHCPRELEASE                 6
DHCPREBIND                  0
DHCPRENEW                   0
DHCPINFORM                  0
```

show ip dhcp configuration

Display the DHCP configuration.

C9000 Series

Syntax `show ip dhcp configuration [global | pool name]`

Parameters

pool *name*	Display the configuration for a DHCP pool.
global	Display the DHCP configuration for the entire system.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# show ip dhcp configuration global

Protocol status        : Enabled
Number of ping packets : 1
Dell#

Dell# show ip dhcp configuration  pool p1

Pool Name            : p1
Pool Type            : Dynamic
Domain Name          : dell.com
Lease Time           : 2Days 0Hrs 0Mins
DNS Servers          : 10.11.0.1
Default Routers      : 1.1.1.1
Network              : 1.1.1.0 255.255.255.0
```

show ip dhcp conflict

Display the address conflict log.

C9000 Series

Syntax `show ip dhcp conflict address`

Parameters

address	Display a particular conflict log entry.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

show ip dhcp lease

Display lease information about the dynamic IP address currently assigned to a DHCP client interface.

C9000 Series

Syntax `show ip dhcp lease [interface type slot/port]`

Parameters

interface *type slot/port*	Enter the keyword `interface` with the interface type and slot/port information to display DHCP lease information for a specified interface. The valid interface types are: • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

show ip dhcp server statistics

Display statistical information about a DHCP server.

C9000 Series

Syntax `show ip dhcp server statistics`

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# show ip dhcp server statistics
Address pools           1
Database agents         0
Automatic bindings      10
Manual bindings         0
Expired bindings        1
Malformed messages      0

Message                 Received
BOOTREQUEST             0
DHCPDISCOVER            10
DHCPREQUEST             16
DHCPDECLINE             0
DHCPRELEASE             8
DHCPINFORM              0

Message                 Sent
BOOTREPLY               0
DHCPOFFER               10
DHCPACK                 16
DHCPNAK                 0
```

Configure Secure DHCP and DHCP Relay

DHCP, as defined by RFC 2131, provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks, including using the switch as a DHCP relay agent.

arp inspection

Enable dynamic arp inspection (DAI) on a VLAN.

C9000 Series

Syntax `arp inspection`

Defaults Disabled

Command Modes INTERFACE VLAN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Introduced on the C-Series and S-Series.

Related Commands arp inspection-trust — specifies a port as trusted so that ARP frames are not validated against the binding table.

arp inspection-trust

Specify a port or an interface as trusted so that ARP frames are not validated against the binding table.

C9000 Series

Syntax `arp inspection-trust`

Defaults Disabled

Command Modes

- INTERFACE
- INTERFACE PORT-CHANNEL
- INTERFACE PORT EXTENDER (conf-if-pegi-*pe-id*/Unit/Port)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Introduced on the C-Series and S-Series.

Related Commands arp inspection — enables dynamic ARP inspection on a VLAN.

clear ip dhcp snooping

Clear the DHCP binding table.

C9000 Series

Syntax `clear ip dhcp snooping binding`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Introduced on the C-Series and S-Series.

Related Commands show ip dhcp snooping — displays the contents of the DHCP binding table.

ip dhcp relay information-option

Enable Option 82.

C9000 Series

Syntax `ip dhcp relay information-option [trust-downstream] [vpn]`

Parameters

trust-downstream Configure the system to trust Option 82 when it is received from the previous-hop router.

vpn Enter the keyword `vpn` to add VPN/VRF related sub-option to relay agent information Option 82.

NOTE: Adds the VPN/VRF related sub-options into the relay agent information option(82). When DHCP broadcasts are forwarded by the relay agent from clients to DHCP server.

Default Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on C-Series and S-Series.

Example

```
Dell(conf)#ip dhcp relay information-option vpn
```

ip dhcp relay source-interface

Configure IPv4 DHCP relay source interface.

Syntax `ip dhcp relay source-interface` *interface*

To disable the IPv4 DHCP relay source interface, use the `no ip dhcp relay source-interface` *interface* command.

Parameters

source-interface *interface* Enter the keyword `source-interface` then the type of interface and the interface information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/plot information.
- For a 10-Gigabit Ethernet information, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet information, enter the keyword `FortyGigabitEthernet` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.
- For a port channel interface, enter thee keyword `port-channel` then a number. The range is from 1 to 128.

- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Disabled

Command Modes
- CONFIGURATION
- INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.0)	Introduced on the C9010, MXL, FN IOM, S3100 series, S4810, S4820T, S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000, S6000–ON, S6010–ON, S6100–ON, and Z9100–ON.

Related Commands
- ipv6 dhcp relay source-interface— Configure DHCP relay source IPv6 interface.

ipv6 dhcp relay source-interface

Configure DHCP relay source IPv6 interface.

Syntax `ipv6 dhcp relay source-interface` *`interface`*

To disable the DHCP relay source IPv6 interface, use the `no ipv6 dhcp relay source-interface` *`interface`* command.

Parameters

source-interface *interface* Enter the keyword `source-interface` then the type of interface and the interface information:
- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/plot information.
- For a 10-Gigabit Ethernet information, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet information, enter the keyword `FortyGigabitEthernet` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.
- For a port channel interface, enter thee keyword `port-channel` then a number. The range is from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Disabled

Command Modes

- CONFIGURATION
- INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.0)	Introduced on the C9010, MXL, FN IOM, S3100 series, S4810, S4820T, S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000, S6000–ON, S6010–ON, S6100–ON, and Z9100–ON.

Related Commands

- ip dhcp relay source-interface— Configure DHCP relay source IP interface.

ip dhcp snooping

Enable DHCP snooping globally.

C9000 Series

Syntax `[no] ip dhcp snooping`

Defaults Disabled

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the S4810 and S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Introduced on the C-Series and S-Series on Layer 2 interfaces.
7.8.1.0	Introduced on the C-Series and S-Series on Layer 3 interfaces.

Usage Information

When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP snooping, the binding table deletes and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.

DHCP snooping supports Layer 3 using DHCP Relay Agent (`ip helper-address`) and Layer 2. You do not have to enable relay agent to snoop on Layer 2 interfaces.

Related Commands ip dhcp snooping vlan — enables DHCP snooping on one or more VLANs.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

Syntax

```
[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address
interface interface-type lease number
```

Parameters

mac *address*	Enter the keyword `mac` then the MAC address of the host to which the server is leasing the IP address.
vlan-id *vlan-id*	Enter the keywords `vlan-id` then the VLAN to which the host belongs. The range is from 2 to 4094.
ip *ip-address*	Enter the keyword `ip` then the IP address that the server is leasing.
interface *type*	Enter the keyword `interface` then the type of interface to which the host is connected: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
lease *time*	Enter the keyword `lease` then the amount of time the IP address are leased. The range is from 1 to 4294967295.

Defaults None

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13(0.0)	Enhanced the command to map multiple IP addresses to one MAC address. Enhanced to support DHCP snooping in a VLT setup.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on the E-Series.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Instructions You can map multiple IP addresses to the same MAC address.

Related Commands

- show ip dhcp snooping — display the contents of the DHCP binding table.

ip dhcp snooping database

Delay writing the binding table for a specified time.

C9000 Series

Syntax `ip dhcp snooping database write-delay minutes`

Parameters

minutes	The range is from 5 to 21600.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping database renew

Renew the binding table.

C9000 Series

Syntax `ip dhcp snooping database renew`

Defaults none

Command Modes
- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping trust

Configure an interface as trusted.

C9000 Series

Syntax `[no] ip dhcp snooping trust`

Defaults **Untrusted**

Command Modes
- INTERFACE
- INTERFACE PORT EXTENDER (conf-if-pegi-p*epe-id* /stack-unit*unit number* /port-id)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping verify mac-address

Validate a DHCP packet's source hardware address against the client hardware address field (CHADDR) in the payload.

C9000 Series

Syntax `[no] ip dhcp snooping verify mac-address`

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.2.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

C9000 Series

Syntax `[no] ip dhcp snooping vlan name`

Parameters

name	Enter the name of a VLAN on which to enable DHCP Snooping.

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information When enabled, the system begins creating entries in the binding table for the specified VLANs.

NOTE: Learning only happens if there is a trusted port in the VLAN.

Related Commands ip dhcp snooping trust — configures an interface as trusted.

ip dhcp source-address-validation

Enable the IP Source Guard.

C9000 Series

Syntax `[no] ip dhcp source-address-validation [ipmac | vlan vlan-id]`

Parameters

ipmac	Enable IP+MAC Source Address Validation.
vlan *vlan-id*	Enable DHCP source address validation on VLAN. Enter the keyword `vlan` and the VLAN identifier (ID). The range is from 1 to 4094.

Defaults Disabled

Command Modes

- INTERFACE
- INTERFACE PORT EXTENDER(conf-if-pegi-pe *pe-id* /stack-unit *unit number* / port-id)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Added the keyword `ipmac`.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

Allocate at least one FP block to `ipmacacl` before you can enable IP+MAC Source Address Validation.

1 Use the `cam-acl l2acl` command from CONFIGURATION mode.
2 Save the running-config to the startup-config.
3 Reload the system.

show ip dhcp binding

Display the DHCP binding table.

C9000 Series

Syntax

```
show ip dhcp binding
```

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell# show ip dhcp binding

IP address      Hardware address   Lease expiration     Type
1.1.1.253       00:00:00:00:00:10  Jan 08 2014 23:57    Automatic
1.1.1.254       00:00:00:00:00:20  Jan 08 2014 23:57    Automatic
```

show ip dhcp snooping

Display the contents of the DHCP binding table or display the interfaces configured with IP Source Guard.

C9000 Series

Syntax

```
show ip dhcp snooping [binding | source-address-validation [discard—counter | interface interface]]
```

Parameters

binding	Display the interfaces configured with IP Source Guard.
source-address-validation	Display the interfaces configured with IP Source Guard.
discard-counter	Display the drop count of the packets.
interface *interface*	Enter the keyword `interface` then type one of the following interface types and slot/port or number information: • For a 1–Gigabit Ethernet interface, enter the keyword `gigabitethernet`. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`. • For a Port Channel interface, enter the keyword `port-channel` then a number. Range is from 1 to 4096. • For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigabitEthernet` then the *pe-id*, stack-unit *unit number*, and *port-id*. The *pe-id* range is 0–255; the stack unit number range is 0–7; and the port—ID range is 0 – 47.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

Related Commands clear ip dhcp snooping — clears the contents of the DHCP binding table.

14

Equal Cost Multi-Path (ECMP)

Equal cost multi-path (ECMP) supports multiple "best paths" in next-hop packet forwarding to a destination device.

ecmp-group

Provides a mechanism to monitor traffic distribution on an ECMP link bundle. A system log is generated when the standard deviation of traffic distribution on a member link exceeds a defined threshold.

C9000 Series

Syntax

`ecmp-group {ecmp-group-id interface interface | link-bundle-monitor}`

To remove the selected interface, use the `ecmp-group no interface` command.

To disable link bundle monitoring, use the `ecmp-group no link-bundle-monitor` command.

Parameters

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

ecmp-group ID	Enter the identifier number for the ECMP group. The range is from 1 to 64.
interface	Enter the following keywords and slot/port to add the interface to the ECMP group: • 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information • For a LAG interface, enter the keywords `port-channel` then the slot/port information. The range is from 1 to 128.

Defaults

Off

Command Modes

- CONFIGURATION
- CONFIGURATION ECMP-GROUP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

Usage Information

Using CONFIGURATION mode, create an ECMP group ID. You can then assign interfaces to the ECMP group using CONFIGURATION ECMP-GROUP mode. You can also enable on the 10–Gigabit Ethernet, 40–Gigabit Ethernet, and port-channel configuration using the CONFIGURATION ECMP-GROUP command mode.

hash-algorithm ecmp

Changes the hash algorithm used to distribute traffic flows across an ECMP.

C9000 Series

Syntax

`hash-algorithm {ecmp {crc16 | crc16cc | crc32MSB | crc32LSB | crc-upper | dest-ip | lsb | xor1 | xor2 | xor4 | xor8 | xor16} hg {crc16 | crc16cc | crc32MSB | crc32LSB | xor1 | xor2 | xor4 | xor8 | xor16} {hg-seed seed-value} lag {crc16 | crc16cc | crc32MSB | crc32LSB | xor1 | xor2 | xor4 | xor8 | xor16} | seed seed-value} linecard slot-id | port-set port-pipe`

To return to the default hash algorithm, use the `no hash-algorithm` command.

To return to the default ECMP hash algorithm, use the `no hash-algorithm ecmp` *algorithm-value* command.

To remove the hash algorithm on a particular line card, use the `no hash-algorithm linecard` *number* command.

Parameters

ecmp *crc16* | *crc16cc* | *crc32MSB* | *crc32LSB* | *crc-upper* | *dest-ip* | *lsb* | *xor1* | *xor2* | *xor4* | *xor8* | *xor16*

Enter the keyword `ecmp` then one of the following options:

- *crc16*: Use CRC16_BISYNC — 16-bit CRC16-bisync polynomial (default)
- *crc16cc*: Use CRC16_CCITT — 16-bit CRC16 using CRC16-CCITT polynomial
- *crc32MSB*: Use CRC32_UPPER — MSB 16 bits of computed CRC32
- *crc32LSB*: Use CRC32_LOWER — LSB 16 bits of computed CRC32
- *crc-upper*: Uses the upper 32 bits of the key for the hash computation
- *dest-ip*: Uses the destination IP for ECMP hashing
- *lsb*: Returns the LSB of the key as the hash
- *xor1*: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1
- *xor2*: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2
- *xor4*: Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4
- *xor8*: Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8

- *xor16*: Use CR16 — 16-bit XOR

hg {*crc16* | *crc16cc* | *crc32MSB* | *crc32LSB* | *xor1* | *xor2* | *xor4* | *xor8* | *xor16*}

Enter the keyword `hg` then one of the following options:

- *crc16*: Use CRC16_BISYNC — 16-bit CRC16-bisync polynomial (default)
- *crc16cc*: Use CRC16_CCITT — 16-bit CRC16 using CRC16-CCITT polynomial
- *crc32MSB*: Use CRC32_UPPER — MSB 16 bits of computed CRC32
- *crc32LSB*: Use CRC32_LOWER — LSB 16 bits of computed CRC32
- *xor1*: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1
- *xor2*: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2
- *xor4*: Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4
- *xor8*: Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8
- *xor16*: Use CR16 — 16-bit XOR

hg-seed *seed-value*

Enter the keywords `hg-seed` then the hash algorithm seed value. The range is from 0 to 2147483646.

lag {*crc16* | *crc16cc* | *crc32MSB* | *crc32LSB* | *xor1* | *xor2* | *xor4* | *xor8* | *xor16*}

Enter the keyword `lag` then one of the following options:

- *crc16*: Use CRC16_BISYNC — 16-bit CRC16-bisync polynomial (default)
- *crc16cc*: Use CRC16_CCITT — 16-bit CRC16 using CRC16-CCITT polynomial
- *crc32MSB*: Use CRC32_UPPER — MSB 16 bits of computed CRC32
- *crc32LSB*: Use CRC32_LOWER — LSB 16 bits of computed CRC32
- *xor1*: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1
- *xor2*: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2
- *xor4*: Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4
- *xor8*: Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8
- *xor16*: Use CR16 — 16-bit XOR

seed *seed-value*

Enter the keyword `seed` then the hash algorithm seed value. The range is from 0 to 2147483646.

linecard *slot-id* | port-set *port-pipe*

Enter the `linecard slot-id` parameters to specify a switch line card. The slot IDs range from 0 to 11.

Enter the `port-set port-pipe` parameters to specify a port pipe (set of ports) on the line card. The port-pipe range is from 0 to 3.

Defaults

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Added the `nh-ecmp` option.
7.7.1.1	Added the `nh-ecmp` option.
6.5.1.0	Added the `line card` option on TeraScale only.
6.3.1.0	Added support for ECMP and LAG on TeraScale only.

Usage Information

To ensure that CRC is not used for LAG, set the default hash-algorithm method.

The hash value calculated with the hash-algorithm command is unique to the entire chassis. The hash algorithm command with the line card option changes the hash for a particular line card by applying the mask specified in the IPSA and IPDA fields.

In addition, the `linecard` *`slot-id`* `ip-sa-mask` *`value`* `ip-da-mask` *`value`* option has the following behavior to maintain bidirectionality:

- When hashing is done on both IPSA and IPDA, the `ip-sa-mask` and `ip-da-mask` values must be equal. (Single Linecard).
- When hashing is done only on IPSA or IPDA, the system maintains bidirectionality with masks set to XX 00 for line card 1 and 00 XX for line card 2 (`ip-sa-mask` and `ip-da-mask`). The mask value must be the same for both line cards when using multiple line cards as ingress (where XX is any value from 00 to FF for both line cards). For example, assume that traffic is flowing between line card 1 and line card 2:
- `hash-algorithm linecard 1 ip-sa-mask aa ip-da-mask 00`
- `hash-algorithm linecard 2 ip-sa-mask 00 ip-da-mask aa`

The different hash algorithms are based on the number of Port Channel members and packet values. The default hash algorithm (number 0) yields the most balanced results in various test scenarios, but if the default algorithm does not provide a satisfactory distribution of traffic, use the hash-algorithm command to designate another algorithm.

When a Port Channel member leaves or is added to the Port Channel, the hash algorithm is recalculated to balance traffic across the members.

hash-algorithm hg

To distribute traffic flows across different internal HiGig links, change the hash algorithm.

C9000 Series

Syntax

```
hash-algorithm hg {crc16 | xor1 | xor2 | xor4 | xor8 | xor16 | crc16cc |
crc32MSB | crc32LSB} linecard slot-id port-set port-pipe
```

Parameters

crc16	Use CRC16_BISYNC — 16-bit CRC16-bisync polynomial (default).
xor1	Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1.
xor2	Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2.
xor4	Use CRC16_BISYNC_AND_XOR4 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor4.
xor8	Use CRC16_BISYNC_AND_XOR8 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor8.
xor16	Use CR16 — 16-bit XOR.
crc16cc	Use CRC16_CCITT — 16-bit CRC16 using CRC16-CCITT polynomial.
crc32MSB	Use CRC32_UPPER — MSB 16 bits of computed CRC32.
crc32LSB	Use CRC32_LOWER — LSB 16 bits of computed CRC32.
linecard *slot-id* port-set *port-pipe*	Enter the linecard slot ID and port-pipe number for the set of ports for which you want to redistribute traffic flows. The range of slot IDs is 0 to 11. The range of port-pipe numbers is 0.

Defaults **crc16 algorithm**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.4	Introduced on the Z9000.

hash-algorithm hg-seed

Select the seed value used in HiGig hashing.

C9000 Series

Syntax `[no] hash-algorithm hg-seed number [linecard slot-id port-set port-pipe]`

Parameters

hg-seed *number*	Enter the keywords `hg-seed` then the hash algorithm seed value. The range is from 0 to 2147483646.
linecard *slot-id* port-set *port-pipe*	(Optional) Enter the line-card slot ID and port-pipe number for the set of ports for which you configure HiGig hashing. The range of slot IDs is 0 to 11. The range of port-pipe numbers is 0.

Defaults **32-bit chassis MAC and system time**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.4	Introduced on the Z9000.

hash-algorithm seed

Select the seed value for the ECMP, LAG, and NH hashing algorithm.

C9000 Series

Syntax `hash-algorithm seed value [linecard slot] [port-set number]`

Parameters

seed *value*	Enter the keyword `seed` then the seed value. The range is from 0 to 4095.
linecard *slot*	Enter the keyword `linecard` then the linecard slot number.
port-set *number*	Enter the keyword `port-set` then the linecard port-pipe number.

Defaults 32–bit Chassis MAC

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the E-Series.

Usage Information

Deterministic ECMP sorts ECMPs in order even though RTM provides them in a random order. However, the hash algorithm uses as a seed the lower 12 bits of the chassis MAC, which yields a different hash result for every chassis. This behavior means that for a given flow, even though the prefixes are sorted, two unrelated chassis select different hops.

The system provides a CLI-based solution for modifying the hash seed to ensure that on each configured system, the ECMP selection is same. When configured, the same seed is set for ECMP, LAG, and NH, and is used for incoming traffic only.

NOTE: While the seed is stored separately on each port-pipe, the same seed is used across all CAMs.

You cannot separate LAG and ECMP but you can use different algorithms across the chassis with the same seed. If LAG member ports span multiple port-pipes and line cards, set the seed to the same value on each port-pipe to achieve deterministic behavior.

If the hash algorithm configuration is removed, the hash seed does not go to the original factory default setting.

ip ecmp-group

Enable and specify the maximum number of ecmp that the L3 CAM hold for a route, By default, when maximum paths are not configured, the CAM can hold a maximum of 16 ecmp per route.

C9000 Series

Syntax

`ip ecmp-group {maximum-paths | {number} {path-fallback}`

To negate a command, use the `no ip ecmp-group maximum-paths {number}` command.

Parameters

maximum-paths	Specify the maximum number of ECMP for a route. The range is 2 to 64.
path-fallback	Use the keywords `path-fallback` to enable this feature. If you enable the feature, re-enter this keyword to disable the feature.

Defaults

16

Command Modes CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.

Usage Information You must save the new ECMP settings to the startup-config (`write-mem`) then reload the system for the new settings to take effect.

Related Commands show ip cam linecard – Display content-addressable memory (CAM) entries for a set of ports on a line card.

ip ecmp weighted

Enables weighted ECMP calculations.

C9000 Series

Syntax `ip ecmp weighted`

To disable weighted ECMP calculations, enter the `no ip ecmp weighted` command.

Defaults N/A

Command Modes CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S-Series.

Usage Information Enabling this CLI would inform the FIB to re-program the destination prefix paths with weights in the HW/CAM on the fly.

If disabled, the CLI would inform the FIB to re-program the destination prefix paths with no weights or regular ECMP.

Example

```
Dell(conf)#ip ecmp ?
weighted                Enables Weighted ECMP
Dell(conf)#ip ecmp weighted
Dell(conf)#do show running-config | grep ecmp
ip ecmp weighted
Dell(conf)#
Dell(conf)#no ip ecmp ?
weighted                Disables Weighted ECMP
Dell(conf)#no ip ecmp weighted
Dell(conf)#do show running-config | grep ecmp
```

link-bundle-distribution trigger-threshold

Provides a mechanism to set the threshold to trigger when traffic distribution begins being monitored on an ECMP link bundle.

C9000 Series

Syntax

`link-bundle-distribution trigger-threshold [percent]`

To exit from ecmp group mode, use the `exit` command.

Parameters

percent	Indicate the threshold value when traffic distribution starts being monitored on an ECMP link bundle. The range is from 1 to 90%. The default is **60%**.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

link-bundle-monitor enable

Provides a mechanism to enable monitoring of traffic distribution on an ECMP link or LAG bundle.

C9000 Series

Syntax

`link-bundle-monitor enable`

To exit from ECMP group mode or Port- Channel mode, use the `exit` command.

Command Modes

- ECMP-GROUP
- PORT-CHANNEL INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

show config

Display the ECMP configuration.

C9000 Series

Syntax `show config`

Command Modes CONFIGURATION-ECMP-GROUP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related Commands show running-config ecmp-group — displays interfaces, LAG, or LAG link bundles being monitored for uneven traffic distribution.

show link-bundle distribution

Display the link-bundle distribution for the interfaces in the bundle, type of bundle (LAG or ECMP), and the most recently calculated interface utilization (either bytes per second rate or maximum rate) for each interface.

C9000 Series

Syntax `show link-bundle-distribution`

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information

In a dual homing setup, you can use this command only from the primary VLT peer.

Example

```
Dell# show link-bundle-distribution
Link-bundle trigger threshold - 60
ECMP bundle - 5 Utilization[In Percent] - 0 Alarm State - Inactive
Interface Line Protocol Utilization[In Percent]
Te 0/4    Up            5
Te 0/3    Up            30
```

15

FCoE Transit

To enable the FCoE Transit feature and configure FIP snooping, use the following Dell Networking Operating System commands on the C9000 platform.

In a converged Ethernet network, a switch can operate as an intermediate Ethernet bridge to snoop on FIP packets during the login process on Fibre Channel over Ethernet (FCoE) forwarders (FCFs). Acting as a transit FIP snooping bridge, the switch uses dynamically created access control lists (ACLs) to permit only authorized FCoE traffic to transmit between an FCoE end-device and an FCF.

Topics:

- clear fip-snooping database interface vlan
- clear fip-snooping statistics
- debug fip snooping
- debug fip snooping rx
- feature fip-snooping
- fip-snooping enable
- fip-snooping fc-map
- fip-snooping max-sessions-per-enodemac
- fip-snooping port-mode fcf
- fip-snooping port-mode fcoe-trusted
- show fip-snooping config
- show fip-snooping enode
- show fip-snooping fcf
- show fip-snooping sessions
- show fip-snooping statistics
- show fip-snooping system
- show fip-snooping vlan

clear fip-snooping database interface vlan

Clear FIP snooping information on a VLAN for a specified FCoE MAC address, ENode MAC address, or FCF MAC address, and remove the corresponding ACLs FIP snooping generates.

C9000 Series

Syntax

```
clear fip-snooping database interface vlan {vlan-id} enode {enode-mac-address}
| fcf {fcf-mac-address} | session {session-mac-address}
```

Parameters

enode-mac-address	Enter the ENode MAC address to be cleared of FIP snooping information.
fcf-mac-address	Enter the FCF MAC address to be cleared of FIP snooping information.

	session-mac-address	Enter the MAC address for the session to be cleared of FIP snooping information.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

clear fip-snooping statistics

Clears the statistics on the FIP packets snooped on all VLANs, a specified VLAN, or a specified port interface.

C9000 Series

Syntax `clear fip-snooping statistics [interface vlan vlan-id | interface port-type port/slot | interface port-channel port-channel-number]`

Parameters

vlan-id	Enter the VLAN ID of the FIP packet statistics to be cleared.
port-type port/slot	Enter the port-type and slot number of the FIP packet statistics to be cleared.
port-channelnumber	Enter the port channel number of the FIP packet statistics to be cleared.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

debug fip snooping

Enable debugging on FIP snooping.

C9000 Series

Syntax `debug fip-snooping [all | acl | error | ifm | info | ipc | tx | rx ]`

Parameters

all	Enter the keyword `all` to enable debugging on all the options.
acl	Enter the keyword `acl` for ACL-specific debugging.
error	Enter the keyword `error` for error-specific debugging.
ifm	Enter the keyword `ifm` for IFM-specific debugging.
info	Enter the keyword `info` for information-specific debugging.
ipc	Enter the keyword `ipc` for IPC-specific debugging.
tx	Enter the keyword `tx` for packet transmit-specific debugging.
rx	Enter the keyword `rx` for packet receive-specific debugging.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.x.x.x	Introduced on the C9000 Series.
9.2(0.2)	Added the `tx` parameter.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

debug fip snooping rx

Enable debugging for FIP snooping receive-specific packets.

C9000 Series

Syntax `debug fip-snooping rx packet-type [all | discovery | virtual-link-instantiation | virtual-link-maintenance| vlan-discovery] [`*`interface`*`]`

Parameters

packet-type	Enter the keyword `packet-type` and then the option type on which to enable debugging. The options are:

- `all` — Enter the keyword `all` to enable debugging on all the options.
- `discovery` — Enter the keyword `discovery` to enable debugging on FCF advertisements and ENode solicitation.
- `virtual-link-instantiation` — Enter the keywords `virtual-link-instantiation` to enable debugging on FLOGI, FDISC, and FLOGO packets.
- `virtual-link-maintenance` — Enter the keywords `virtual-link-maintenance` to enable debugging on FIP clear virtual link frames and keepalives.
- `vlan-discovery` — Enter the keywords `vlan-discovery` to enable debugging on VLAN requests and notifications.

interface Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(0.2)	Introduced on the S4810 and S4820T. Added the receive parameters `packet-type` and `interfaces` and their options.

feature fip-snooping

Enable FCoE transit and FIP snooping on a switch.

C9000 Series

Syntax `feature fip-snooping`

To disable the FCoE transit feature, use the `no feature fip-snooping` command.

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

fip-snooping enable

Enable FIP snooping on all VLANs or on a specified VLAN.

C9000 Series

Syntax

`fip-snooping enable`

To disable the FIP snooping feature on all or a specified VLAN, use the `no fip-snooping enable` command.

Defaults

FIP snooping is disabled on all VLANs.

Command Modes

- CONFIGURATION
- VLAN INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Information

The maximum number of FCFs supported per FIP snooping-enabled VLAN is twelve. The maximum number of FIP snooping sessions supported per ENode server is 32 by default. You can configure up to 64 sessions.

fip-snooping fc-map

Configure the FC-MAP value FIP snooping uses on all VLANs.

C9000 Series

Syntax

`fip-snooping fc-map` *`fc-map-value`*

To return the configured FM-MAP value to the default value, use the `no fip-snooping fc-map` command.

Parameters

fc-map-value Enter the FC-MAP value FIP snooping uses. The range is from 0EFC00 to 0EFCFF.

Defaults **0x0EFC00**

Command Modes

- CONFIGURATION
- VLAN INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

fip-snooping max-sessions-per-enodemac

Configure the maximum session limit per ENode MAC address.

C9000 Series

Syntax `fip-snooping max-sessions-per-enode-mac` *`max-sessions-value`*

To return the configured maximum sessions to the default value, use the `no fip-snooping max-sessions-per-enode-mac` command.

Parameters

max-sessions-value Enter the maximum number of sessions allowed per ENode MAC address. The range is from 1 to 64.

Defaults **32**

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(0.2)	Introduced on the S4810 and S4820T.

fip-snooping port-mode fcf

Configure the port for bridge-to-FCF links.

C9000 Series

Syntax

`fip-snooping port-mode fcf`

To disable the bridge-to-FCF link on a port, use the `no fip-snooping port-mode fcf` command.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Information

The maximum number of FCFs supported per FIP snooping-enabled VLAN is twelve.

NOTE: The `fip-snooping port-mode fcf` command is not supported on cascade interfaces or extended ports.

fip-snooping port-mode fcoe-trusted

Configure the port for bridge-to-bridge links.

C9000 Series

Syntax

`fip-snooping port-mode fcoe-trusted`

To remove the bridge-to-bridge link configuration from the port, use the `no fip-snooping port-mode fcoe-trusted` command.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on MXL 10/40GbE Switch IO Module.

Usage Information The maximum number of FCoE VLANs supported on the switch is eight.

NOTE: This command is not supported on cascade interfaces or extended ports.

show fip-snooping config

Display the FIP snooping status and configured FC-MAP values.

C9000 Series

Syntax
```
show fip-snooping config
```

Command Modes
- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example
```
Dell# show fip-snooping config
FIP Snooping Feature enabled Status: Enabled
FIP Snooping Global enabled Status: Enabled
Global FC-MAP Value: 0X0EFC00

FIP Snooping enabled VLANs
VLAN    Enabled    FC-MAP
----    -------    --------
100     TRUE       0X0EFC00
```

show fip-snooping enode

Display information on the ENodes in FIP-snooped sessions, including the ENode interface and MAC address, FCF MAC address, VLAN ID and FC-ID.

C9000 Series

Syntax

```
show fip-snooping enode [enode-mac enode-mac-address]
```

Parameters

enode-mac-address	Enter the MAC address of the ENodes to display.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Inroduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Information

The following describes the `show fip-snooping enode` command shown in the following example.

Field	Description
ENode MAC	MAC address of the ENode.
ENode Interface	Slot/ port number of the interface connected to the ENode.
FCF MAC	MAC address of the FCF.
VLAN	VLAN ID number the session uses.
FC-ID	Fibre Channel session ID the FCF assigns.

Example

```
Dell# show fip-snooping enode
Enode MAC         Enode Interface FCF MAC           VLAN FC-ID
--------- --------------- ------- ---- -----
d4:ae:52:1b:e3:cd Te 0/11         54:7f:ee:37:34:40 100 62:00:11
```

show fip-snooping fcf

Display information on the FCFs in FIP-snooped sessions, including the FCF interface and MAC address, FCF interface, VLAN ID, FC-MAP value, FKA advertisement period, and number of ENodes connected.

C9000 Series

Syntax

```
show fip-snooping fcf [fcf-mac fcf-mac-address]
```

Parameters

fcf-mac-address	Enter the MAC address of the FCF to display.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Information

The following describes the `show fip-snooping fcf` command shown in the following example.

Field	Description
FCF MAC	MAC address of the FCF.
FCF Interface	Slot/port number of the interface to which the FCF is connected.
VLAN	VLAN ID number the session uses.
FC-MAP	FC-Map value the FCF advertises.
ENode Interface	Slot/ number of the interface connected to the ENode.
FKA_ADV_PERIOD	Time (in milliseconds) during which FIP keep-alive advertisements transmit.
No of ENodes	Number of ENodes connected to the FCF.
FC-ID	Fibre Channel session ID the FCF assigns.

Example

```
Dell# show fip-snooping fcf
FCF MAC        FCF Interface VLAN FC-MAP FKA_ADV_PERIOD No. of Enodes
-------- ------------- ---- ------ -------------- -------------
54:7f:ee:37:34:40 Po 22      100 0e:fc:00 4000                2
```

show fip-snooping sessions

Display information on FIP-snooped sessions on all VLANs or a specified VLAN, including the ENode interface and MAC address, the FCF interface and MAC address, VLAN ID, FCoE MAC address and FCoE session ID number (FC-ID), worldwide node name (WWNN) and the worldwide port name (WWPN).

C9000 Series

Syntax `show fip-snooping sessions [interface vlan vlan-id]`

Parameters

vlan-id	Enter the vlan-id of the specified VLAN to display.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Information

The following describes the `show fip-snooping sessions` command shown in the following example.

Field	Description
ENode MAC	MAC address of the ENode.
ENode Interface	Slot/ port number of the interface connected to the ENode.
FCF MAC	MAC address of the FCF.
FCF Interface	Slot/ port number of the interface to which the FCF is connected.
VLAN	VLAN ID number the session uses.
FCoE MAC	MAC address of the FCoE session the FCF assigns.
FC-ID	Fibre Channel ID the FCF assigns.
Port WWPN	Worldwide port name of the CNA port.
Port WWNN	Worldwide node name of the CNA port.

Example

```
Dell# show fip-snooping sessions
Enode MAC         Enode Intf  FCF MAC          FCF Intf VLAN   FCoE MAC
FC-ID      Port WWPN              Port WWNN
---------         ----------  -------          -------- ----   --------
-----      ---------              ---------
```

```
aa:bb:cc:00:00:00 Te 10/0   aa:bb:cf:00:00:00 Te 10/1   2    0e:fc:00:01:00:02
01:00:02 31:00:0e:fc:00:00:00:00  21:00:0e:fc:00:00:00:00
aa:bb:cd:00:00:00 Te 11/0   aa:bb:cf:00:00:00 Te 10/1   2    0e:fc:00:01:00:01
01:00:01 31:00:0e:fc:00:00:00:01  21:00:0e:fc:00:00:00:01
aa:bb:ce:00:00:00 Te 2/0    aa:bb:cf:00:00:00 Te 10/1   2    0e:fc:00:01:00:03
01:00:03 31:00:0e:fc:00:00:00:02  21:00:0e:fc:00:00:00:02
```

```
Dell# show fip-snooping sessions
Enode MAC Enode Intf FCF MAC FCF Intf VLAN FCoE MAC
 FC-ID Port WWPN
    Port WWNN
-----------------------------------------------
00:00:c9:f1:e1:37 Te 0/28 54:7f:ee:34:77:4e Te 1/47 111
  0e:fc:00:b5:00:07 b5:00:07 10:00:00:00:c9:f1:e1:37
     20:00:00:00:c9:f1:e1:37
00:c0:dd:12:c0:05 Te 1/26 54:7f:ee:34:77:4e Te 1/47 111
  0e:fc:00:b5:00:75 b5:00:75 21:00:00:c0:dd:12:c0:05
    20:00:00:c0:dd:12:c0:05
```

show fip-snooping statistics

Display statistics on the FIP packets snooped on all interfaces, including VLANs, physical ports, and port channels.

C9000 Series

Syntax

```
show fip-snooping statistics [interface vlan vlan-id | interface port-type
port/slot | interface port-channel port-channel-number]
```

Parameters

vlan-id	Enter the VLAN ID of the FIP packet statistics displays.
port-type port/slot	Enter the port-type and slot number of the FIP packet statistics displays.
port-channel-number	Enter the port channel number of the FIP packet statistics displays.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Information

The following describes the `show fip-snooping statistics` command shown in the following example.

Field	Description
Number of VLAN Requests	Number of FIP-snoop VLAN request frames received on the interface.
Number of VLAN Notifications	Number of FIP-snoop VLAN notification frames received on the interface.
Number of Multicast Discovery Solicits	Number of FIP-snoop multicast discovery solicit frames received on the interface.
Number of Unicast Discovery Solicits	Number of FIP-snoop unicast discovery solicit frames received on the interface.
Number of FLOGI	Number of FIP-snoop FLOGI request frames received on the interface.
Number of FDISC	Number of FIP-snoop FDISC request frames received on the interface.
Number of FLOGO	Number of FIP-snoop FLOGO frames received on the interface
Number of ENode Keep Alives	Number of FIP-snoop ENode keep-alive frames received on the interface.
Number of VN Port Keep Alives	Number of FIP-snoop VN port (Virtual N-port) keep-alive frames received on the interface
Number of Multicast Discovery Advertisements	Number of FIP-snoop multicast discovery advertisements received on the interface.
Number of Unicast Discovery Advertisements	Number of FIP-snoop unicast discovery advertisements received on the interface.
Number of FLOGI Accepts	Number of FIP FLOGI accept frames received on the interface.
Number of FLOGI Rejects	Number of FIP FLOGI reject frames received on the interface.
Number of FDISC Accepts	Number of FIP FDISC accept frames received on the interface.
Number of FDISC Rejects	Number of FIP FDISC reject frames received on the interface.
Number of FLOGO Accepts	Number of FIP FLOGO accept frames received on the interface.
Number of FLOGO Rejects	Number of FIP FLOGO reject frames received on the interface.
Number of CVLs	Number of FIP clear virtual link frames received on the interface.
Number of FCF Discovery Timeouts	Number of FCF discovery timeouts that occurred on the interface.
Number of VN Port Session Timeouts	Number of VN port session timeouts that occurred on the interface.
Number of Session failures due to Hardware Config	Number of session failures due to hardware configuration that occurred on the interface.

Example

```
Dell# show fip-snooping statistics interface vlan 100
Number of Vlan Requests                :0
Number of Vlan Notifications           :0
Number of Multicast Discovery Solicits :2
Number of Unicast Discovery Solicits   :0
Number of FLOGI                        :2
Number of FDISC                        :16
Number of FLOGO                        :0
Number of Enode Keep Alive             :9021
Number of VN Port Keep Alive           :3349
Number of Multicast Discovery Advertisement :4437
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts                :2
Number of FLOGI Rejects                :0
Number of FDISC Accepts                :16
Number of FDISC Rejects                :0
Number of FLOGO Accepts                :0
Number of FLOGO Rejects                :0
Number of CVL                          :0
Number of FCF Discovery Timeouts       :0
Number of VN Port Session Timeouts     :0
Number of Session failures due to Hardware Config :0
Dell(conf)#

Dell# show fip-snooping statistics int tengigabitethernet 0/11
Number of Vlan Requests                :1
Number of Vlan Notifications           :0
Number of Multicast Discovery Solicits :1
Number of Unicast Discovery Solicits   :0
Number of FLOGI                        :1
Number of FDISC                        :16
Number of FLOGO                        :0
Number of Enode Keep Alive             :4416
Number of VN Port Keep Alive           :3136
Number of Multicast Discovery Advertisement :0
Number of Unicast Discovery Advertisement :0
Number of FLOGI Accepts                :0
Number of FLOGI Rejects                :0
Number of FDISC Accepts                :0
Number of FDISC Rejects                :0
Number of FLOGO Accepts                :0
Number of FLOGO Rejects                :0
Number of CVL                          :0
Number of FCF Discovery Timeouts       :0
Number of VN Port Session Timeouts     :0
Number of Session failures due to Hardware Config :0
```

Example (Port Channel)

```
Dell# show fip-snooping statistics interface port-channel 22
Number of Vlan Requests                :0
Number of Vlan Notifications           :2
Number of Multicast Discovery Solicits :0
Number of Unicast Discovery Solicits   :0
Number of FLOGI                        :0
Number of FDISC                        :0
Number of FLOGO                        :0
Number of Enode Keep Alive             :0
Number of VN Port Keep Alive           :0
Number of Multicast Discovery Advertisement :4451
Number of Unicast Discovery Advertisement :2
Number of FLOGI Accepts                :2
Number of FLOGI Rejects                :0
Number of FDISC Accepts                :16
Number of FDISC Rejects                :0
Number of FLOGO Accepts                :0
Number of FLOGO Rejects                :0
Number of CVL                          :0
Number of FCF Discovery Timeouts       :0
```

```
Number of VN Port Session Timeouts     :0
Number of Session failures due to Hardware Config :0
```

show fip-snooping system

Display information on the status of FIP snooping on the switch (enabled or disabled), including the number of FCoE VLANs, FCFs, ENodes, and currently active sessions.

C9000 Series

Syntax

```
show fip-snooping system
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example

```
Dell# show fip-snooping system
Global Mode : Enabled
FCOE VLAN List (Operational) : 1, 100
FCFs                         : 1
Enodes                       : 2
Sessions                     : 17
```

show fip-snooping vlan

Display information on the FCoE VLANs on which FIP snooping is enabled.

C9000 Series

Syntax

```
show fip-snooping vlan
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example

```
Dell# show fip-snooping vlan
* = Default VLAN
VLAN FC-MAP    FCFs Enodes Sessions
---- ------ ---- ------ --------
*1    -        -    -      -
100   0X0EFC00 1    2      17
```

16

FIPS Cryptography

To configure federal information processing standards (FIPS) cryptography, use the commands described in this chapter.

Topics:

- fips mode enable
- show fips status
- show ip ssh
- ssh

fips mode enable

Enable the FIPS cryptography mode on the platform.

C9000 Series

Syntax

```
[no] fips mode enable
```

To disable the FIPS cryptography mode, use the `no fips mode enable` command.

Default

Disabled

Command Modes

CONFIGURATION

Example

```
Dell(conf)#fips mode enable
WARNING: Enabling FIPS mode will close all SSH/Telnet connection, restart
those servers, and destroy all configured host keys.
proceed (y/n) ? y
Dell(conf)#
```

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.1(0.0)	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

show fips status

Displays the status of the FIPS mode.

C9000 Series

Syntax `show fips status`

Defaults None

Command Modes EXEC

Example

```
Dell#show fips status
FIPS Mode: Enabled
Dell#
```

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.1(0.0)	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

show ip ssh

Display information about established SSH sessions

C9000 Series

Syntax `show ip ssh`

Defaults none

Command Modes EXEC
EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Removed the support for hmac-sha2-256-96 algorithm.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.1(0.0)	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example

```
Dell# show ip ssh
SSH server                : enabled.
SSH server version        : v1 and v2.
SSH server vrf            : default.
SSH server ciphers        : aes256-ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-
ctr,aes128-cbc,3des-cbc.
SSH server macs           : hmac-sha2-256,hmac-sha1,hmac-sha1-96,hmac-md5,hmac-
md5-96.
SSH server kex algorithms : diffie-hellman-group-exchange-sha1,diffie-hellman-
group1-sha1,diffie-hellman-group14-sha1.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA       Authentication  : disabled.
   Vty          Encryption      HMAC            Remote IP
   0            aes128-ctr      hmac-md5        10.16.150.185
```

With FIPS Mode enabled:

```
Dell#show ip ssh
SSH server                : enabled.
SSH server version        : v2.
SSH server vrf            : default.
SSH server ciphers        : aes256-ctr,aes256-cbc,aes192-ctr,aes192-cbc,aes128-
ctr,aes128-cbc,3des-cbc.
SSH server macs           : hmac-sha2-256,hmac-sha1,hmac-sha1-96.
SSH server kex algorithms : diffie-hellman-group14-sha1.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA       Authentication  : disabled.
   Vty          Encryption      HMAC            Remote IP
   0            aes128-ctr      hmac-sha1       10.16.150.185
Dell(conf)#
```

ssh

Open an SSH connection specifying the hostname, username, port number, and version of the SSH client.

C9000 Series

Syntax

```
ssh {hostname|ipv4 address|ipv6 address} [-c encryption cipher|-l username|-m
HMAC alogorithm|-p port-number|-v {1|2}]
```

Parameters

hostname	(OPTIONAL) Enter the IP address or the hostname of the remote device.
ipv4 address	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.

ipv6 addressprefix (OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

-c encryption cipher Enter the following encryption cipher to use. (For v2 clients only.)
Without the FIPS mode enabled:

- `aes256-ctr` : Force ssh to use the aes256-ctr encryption cipher.
- `aes256-cbc` : Force ssh to use the aes256-cbc encryption cipher.
- `aes192-ctr` : Force ssh to use the aes192-ctr encryption cipher.
- `aes192-cbc` : Force ssh to use the aes192-cbc encryption cipher.
- `aes128-ctr` : Force ssh to use the aes192-ctr encryption cipher.
- `aes128-cbc` : Force ssh to use the aes192-cbc encryption cipher.
- `3des-cbc` : Force ssh to use 3des-cbc encryption cipher.

With the FIPS mode enabled:

- `aes256-ctr` : Force ssh to use the aes256-ctr encryption cipher.
- `aes256-cbc` : Force ssh to use the aes256-cbc encryption cipher.
- `aes192-ctr` : Force ssh to use the aes192-ctr encryption cipher.
- `aes192-cbc` : Force ssh to use the aes192-cbc encryption cipher.
- `aes128-ctr` : Force ssh to use the aes192-ctr encryption cipher.
- `aes128-cbc` : Force ssh to use the aes192-cbc encryption cipher.
- `3des-cbc` : Force ssh to use 3des-cbc encryption cipher.

-l username (OPTIONAL) Enter the keyword `–l` then the user name used in this SSH session. The default is the user name of the user associated with the terminal.

-m HMAC algorithm Enter one of the following HMAC algorithms to use. (For v2 clients only.):
Without the FIPS mode enabled:

- `hmac-sha2-256` : Force ssh to use the hmac-sha2-256 HMAC algorithm.
- `hmac-sha1`: Force ssh to use the hmac-sha1 HMAC algorithm.
- `hmac-sha1-96`: Force ssh to use the hmac-sha1–96 HMAC algorithm.
- `hmac-md5`: Force ssh to use the hmac-md5 HMAC algorithm.
- `hmac-md5-96`: Force ssh to use the hmac-md5–96 HMAC algorithm.

With the FIPS mode enabled:

- `hmac-sha2-256` : Force ssh to use the hmac-sha2-256 HMAC algorithm.
- `hmac-sha1`: Force ssh to use the hmac-sha1 HMAC algorithm.
- `hmac-sha1-96`: Force ssh to use the hmac-sha1–96 HMAC algorithm.

-p port-number (OPTIONAL) Enter the keyword `–p` then the port number.
The range is 1 to 65536

The default is 22

-v {1|2} (OPTIONAL) Enter the keyword `–v` then the SSH version 1 or 2.
The default: The version from the protocol negotiation.

NOTE: If the FIPS mode is enabled, this option does not display in the output.

Defaults As indicated above.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Removed the support for hmac-sha2-256-96 algorithm.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.1(0.0)	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Related Commands

ip ssh server	Configure an SSH server.
show ip ssh client-pub-keys	Display the client-public keys.

Usage Information Both inbound and outbound SSH sessions using IPv4 or IPv6 addressing are supported. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

Example

If FIPS mode is not enabled:

```
Dell#ssh 10.11.8.12 ?
-c                      Encryption cipher to use (for v2 clients only)
-l                      User name option
-m                      HMAC algorithm to use (for v2 clients only)
-p                      SSH server port option (default 22)
-v                      SSH protocol version
<cr>
Dell#ssh 10.11.8.12 -c ?
3des-cbc                Force ssh to use 3des-cbc encryption cipher
aes128-cbc              Force ssh to use aes128-cbc encryption cipher
aes192-cbc              Force ssh to use aes192-cbc encryption cipher
aes256-cbc              Force ssh to use aes256-cbc encryption cipher
aes128-ctr              Force ssh to use aes128-ctr encryption cipher
aes192-ctr              Force ssh to use aes192-ctr encryption cipher
aes256-ctr              Force ssh to use aes256-ctr encryption cipher

Dell#ssh 10.11.8.12 -m ?
hmac-md5                Force ssh to use hmac-md5 HMAC algorithm
hmac-md5-96             Force ssh to use hmac-md5-96 HMAC algorithm
hmac-sha1               Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96            Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-sha2-256           Force ssh to use hmac-sha2-256 HMAC algorithm
```

With FIPS mode enabled:

```
Dell#ssh 10.11.8.12 ?
-c                      Encryption cipher to use (for v2 clients only)
-l                      User name option
-m                      HMAC algorithm to use (for v2 clients only)
-p                      SSH server port option (default 22)
<cr>

Dell#ssh 10.11.8.12 -c ?
3des-cbc                Force ssh to use 3des-cbc encryption cipher
aes128-cbc              Force ssh to use aes128-cbc encryption cipher
aes192-cbc              Force ssh to use aes192-cbc encryption cipher
aes256-cbc              Force ssh to use aes256-cbc encryption cipher
aes128-ctr              Force ssh to use aes128-ctr encryption cipher
aes192-ctr              Force ssh to use aes192-ctr encryption cipher
aes256-ctr              Force ssh to use aes256-ctr encryption cipher

Dell#ssh 10.11.8.12 -m ?
hmac-sha1               Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96            Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-sha2-256           Force ssh to use hmac-sha2-256 HMAC algorithm
```

17

Flex Hash and Optimized Boot-Up

This chapter describes the Flex Hash and fast-boot enhancements.

Topics:

- encapsulation dot1q
- lacp fast-switchover
- load-balance flexhash
- load-balance ingress-port enable

encapsulation dot1q

Configures lite-subinterfaces. This command is supported on the S6000 platform.

Syntax

`encapsulation dot1q` *`vlan-id`*

To remove a previously configured lite-subinterface, use the `no` version of this command.

Parameters

dot1q *vlan-id*	Enter the keyword `dot1q` followed by the VLAN ID to which the host belongs. The range is from 1 to 4094. A lite subinterface is considered as a Layer 3 port property and is synchronous with the existing rules of applying Layer 2 or Layer 3 properties to an interface.

Command Modes

INTERFACE

Command History

Version	
9.9(0.0)	Introduced on the C9010.
9.3.0.0	Introduced on the S6000 platform.

Usage Information

To enable routing of RRoCE packets, the VLAN ID is mapped to the default VLAN ID of 4095 and this mapping is performed using VLAN translation. After VLAN translation, the RRoCE packets are considered in the same manner as normal IP packets that are received on Layer 3 interface and routed in the egress direction. At the egress interface, the VLAN ID is appended to the packet and transmitted out of the interface as a tagged packet with the dot1Q value preserved. The dot1Q value is preserved only for egress interfaces that are associated with a VLAN or a lite-subinterface . If a Layer 3 interface is configured without the encapsulation 802.1Q VLAN ID or is an untagged interface in a VLAN , the dot1Q value is not preserved .

lacp fast-switchover

Cause the physical ports to be aggregated faster by configuring this capability in a port-channel on both the nodes that are members of a port-channel.

C9000 Series

Syntax

`lacp fast-switchover`

To disable the capability of faster aggregation of the member ports of a LAG or a port-channel bundle, use the no version of this command.

Defaults

Not configured

Command Modes

INTERFACE (conf-if-po-number)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.3(0.0)	Introduced on the S6000.

Usage Information

You can configure the optimal switchover functionality for LACP even if you do not enable the fast boot mode on the system. You must configure the long timeout mechanism for the LACP session to enable the fast boot capability to operate properly. This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, this command has no effect

If you configure the optimized booting-time capability and perform a reload of the system, the LACP application sends PDUs across all the active LACP links immediately.

Related Commands

show lacp — displays the LACP configuration.

load-balance flexhash

Specify the parameters for the Flex Hash mechanism, such as whether IPv4 or IPv6 packets must be subject to Flex Hash functionality, a unique protocol number, the offset of hash fields from the start of the L4 header to be used for hash calculation, and a meaningful description to associate the protocol number with the name. This utility is supported on the platform.

Syntax

`load-balance flexhash ipv4/ipv6 ip-proto <protocol number> <description string> offset1 <offset1 value> [offset2 <offset2 value>]`

To disable the Flex hash settings, use the `no load-balance flexhash ipv4/ipv6 ip-proto protocol number` command.

Parameters

ipv4	Denotes whether Flex Hash needs to be enabled for IPv4 packets.
ipv6	Denotes whether Flex Hash needs to be enabled for IPv6 packets.
protocol number	Represents the Outer IPv4 protocol field in case of IPv4 packets, and the Outer IPv6 next header field in case of IPv6 packets. The `ipv4/ipv6` keyword and the IP protocol value are used as keys to identify if a duplicate flex hash configuration is already present. Duplicate flex hash configuration is not possible. To change an existing flex hash

configuration, you must delete the existing flex hash attribute and configure the flex attribute afresh.

description string	A description string is followed by the protocol number to enable you to associate the protocol number with the protocol name in an easily-identifiable way. For example, for a protocol number of 254, you can specify the description as RRoCE.
offset1 *value*	Specify the byte offset from the start of the L4 header from which the 2-byte data is extracted and be used in hash computation. You must enter the offset as an even number. The offset range is 0 – 30 bytes from start of L4 header.
offset2 *value*	(Optional) Specify the additional 2 bytes that must be extracted from the start of the L4 header to be used for hash computation. You must enter the offset as an even number. The offset range is 0 – 30 bytes from start of L4 header.

Default None

Command Modes CONFIGURATION mode

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.3(0.0)	Introduced on the S6000 platform.

Usage Information With the introduction of various overlay technologies such as network virtualization using generic routing encapsulation (NVGRE) segments and Routable Remote Direct Memory Access (RRDMA) over Converged Ethernet (RRoCE), information related to a traffic flow is contained in the L4 header. The fields in the L2 and L3 headers are not sufficient to distinguish the flows. Therefore, the fields in the L4 header are processed when hashing is performed for packets over LAG and ECMP links. The Flex Hash functionality enables you to configure a packet search key and matches packets based on the search key. When a packet matches the search key, two 16-bit hash fields are extracted from the start of the L4 header and provided as inputs (bins 2 and 3) for RTAG7 hash computation. You must specify the offset of hash fields from the start of the L4 header, which contains a flow identification field.

You can cause the system to include the fields present at the offsets that you define (from the start of the L4 header) as a part of LAG and ECMP computation. Also, you can specify whether the IPv4 or IPv6 packets must be operated with the Flex Hash mechanism.

Example

```
Dell(conf)# load-balance flexhash ipv4 ip-proto 1 desc offset1 1 offset2 2
```

load-balance ingress-port enable

Enable the Flex hash functionality. This utility is supported on the C9000 platform.

Syntax

```
load-balance ingress-port enable
```

To disable the Flex hash capability, use the **no** version of this command.

Default None

Command Modes CONFIGURATION mode

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9.(0.0)	Introduced on the C9010.
9.3(0.0)	Introduced on the S6000 platform.

Usage Information

Flex hash uses the RTAG7 bins 2 and 3 (overlay bins). These bins must be enabled for Flex hash to be configured. These bins contain the source module and source port information. These bins are disabled by default in releases of Dell Networking OS earlier than Release 9.3.0.0. The default behavior of disabling of these bins occurs because of incorrect egress port information that would otherwise be displayed in the output of the diagnostic show command of `show ip flow`.

As a result, when load balancing of RRoCE packets using Flex hash is enabled, the `show ip flow` command is not functional. Similarly, when `show ip flow` command operates (ingress port based load balancing is disabled) the hashing of RRoCE packets is not operational.

Flex hash APIs do not mask out unwanted byte values after extraction of the data from the Layer 4 headers for the offset value.

Example

```
Dell#load-balance ingress-port enable
```

18

Force10 OS Resilient Ring Protocol (FRRP)

Force10 OS resilient ring protocol (FRRP) is a proprietary protocol for that offers fast convergence in a Layer 2 network without having to run the spanning tree protocol (STP).

The resilient ring protocol is an efficient protocol that transmits a high-speed token across a ring to verify the link status. All the intelligence is contained in the master node with practically no intelligence required of the transit mode.

Important Points to Remember

- FRRP is media- and speed-independent.
- FRRP is a Dell Networking proprietary protocol that does not interoperate with any other vendor.
- Spanning Tree must be disabled on both primary and secondary interfaces before Resilient Ring protocol is enabled.
- A VLAN configured as the control VLAN for a ring cannot be configured as a control or member VLAN for any other ring.
- Member VLANs across multiple rings are not supported in Master nodes.
- If multiple rings share one or more member VLANs, they cannot share any links between them.
- Each ring can have only one Master node; all others are Transit nodes.
- FRRP is not supported on port extender (PE) ports.

Topics:

- clear frrp
- debug frrp
- description
- disable
- interface
- member-vlan
- mode
- protocol frrp
- show frrp
- timer

clear frrp

Clear the FRRP statistics counters.

C9000 Series

Syntax `clear frrp [ring-id]`

Parameters

ring-id (Optional) Enter the ring identification number. The range is from 1 to 255.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.5.1.0	Introduced.

Usage Information Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. The system requires a command line confirmation before the command executes. This command clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

Example

```
Dell# clear frrp

Clear frrp statistics counter on all ring [confirm] yes

Dell#clear frrp 4

Clear frrp statistics counter for ring 4 [confirm] yes

Dell#
```

Related Commands show frrp — displays the Resilient Ring Protocol configuration.

debug frrp

Clear the FRRP statistics counters.

C9000 Series

Syntax `debug frrp {event | packet | detail} [ring-id] [count number]`

To disable debugging, use the `no debug frrp {event | packet | detail} {ring-id} [countnumber]` command.

Parameters

event Enter the keyword `event` to display debug information related to ring protocol transitions.

packet	Enter the keyword `packet` to display brief debug information related to control packets.
detail	Enter the keyword `detail` to display detailed debug information related to the entire ring protocol packets.
ring-id	(Optional) Enter the ring identification number. The range is from 1 to 255.
count *number*	Enter the keyword `count` then the number of debug outputs. The range is from 1 to 65534.

Defaults Disabled.

Command Modes CONFIGURATION (conf-frrp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

Usage Information Because the resilient ring protocol can potentially transmit 20 packets per interface, restrict debug information.

description

Enter an identifying description of the ring.

C9000 Series

Syntax `description *Word*`

To remove the ring description, use the `no description [*Word*]` command.

Parameters

Word	Enter a description of the ring. Maximum: 255 characters.

Defaults none

Command Modes CONFIGURATION (conf-frrp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

disable

Disable the resilient ring protocol.

C9000 Series

Syntax

`disable`

To enable the Resilient Ring Protocol, use the `no disable` command.

Defaults

Disabled

Command Modes

CONFIGURATION (conf-frrp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

interface

Configure the primary, secondary, and control-vlan interfaces.

C9000 Series

Syntax

`interface {primary interface secondary interface control-vlan vlan-id}`

To return to the default, use the `no interface {primary interface secondary interface control-vlan vlan-id}` command.

Parameters

primary *interface*

Enter the keyword `primary` to configure the primary interface then one of the following interfaces and slot/port information:

- `Fast Ethernet interface`: enter the keyword `FastEthernet` then the slot/port information.
- `Port Channel interface`: enter the keyword `port-channel` then a number. The range is from 1 to 128.
- `10-Gigabit Ethernet interface`: enter the keyword `TenGigabitEthernet` then the slot/port information
- `40-Gigabit Ethernet interface`: enter the keyword `fortyGigE` then the slot/port information

secondary *interface*

Enter the keyword `secondary` to configure the secondary interface then one of the following interfaces and slot/port information:

- `Fast Ethernet interface`: enter the keyword `FastEthernet` then the slot/port information.
- `Port Channel interface`: enter the keyword `port-channel` then a number. The range is from 1 to 128.
- `10-Gigabit Ethernet interface`: enter the keyword `TenGigabitEthernet` then the slot/port information
- `40-Gigabit Ethernet interface`: enter the keyword `fortyGigE` then the slot/port information

control-vlan *vlan-id*

Enter the keyword `control-vlan` then the VLAN ID. The range is from 1 to 4094.

Defaults

none

Command Modes

CONFIGURATION (conf-frrp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

Usage Information This command causes the Ring Manager to take ownership of the two ports after IFM validates the configuration. Ownership is relinquished for a port only when the interface does not play a part in any control VLAN, that is, the interface does not belong to any ring.

Related Commands show frrp — displays the Resilient Ring Protocol configuration information.

member-vlan

Specify the member VLAN identification numbers.

C9000 Series

Syntax `member-vlan {vlan-range}`

To return to the default, use the `no member-vlan [vlan-range]` command.

Parameters

vlan-range	Enter the member VLANs using VLAN IDs (separated by commas), a range of VLAN IDs (separated by a hyphen), a single VLAN ID, or a combination. For example: VLAN IDs (comma-separated): 3, 4, 6. Range (hyphen-separated): 5-10. Combination: 3, 4, 5-10, 8.

Defaults none

Command Modes CONFIGURATION (conf-frrp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

mode

Set the Master or Transit mode of the ring.

C9000 Series

Syntax

`mode {master | transit}`

To reset the mode, use the `no mode {master | transit}` command.

Parameters

master	Enter the keyword `master` to set the Ring node to Master mode.
transit	Enter the keyword`transit` to set the Ring node to Transit mode.

Defaults

Mode None

Command Modes

CONFIGURATION (conf-frrp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

protocol frrp

Enter the Resilient Ring Protocol and designate a ring identification.

C9000 Series

Syntax

`protocol frrp {`*`ring-id`*`}`

To exit the ring protocol, use the `no protocol frrp {`*`ring-id`*`}` command.

Parameters

ring-id	Enter the ring identification number. The range is from 1 to 255.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced

Usage Information This command places you into the resilient ring protocol. After executing this command, the command line prompt changes to `conf-frrp`.

show frrp

Display the resilient ring protocol configuration.

C9000 Series

Syntax `show frrp [ring-id [summary]] | [summary]`

Parameters

ring-id	Enter the ring identification number. The range is from 1 to 255
summary	(OPTIONAL) Enter the keyword `summary` to view just a summarized version of the Ring configuration.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

Usage Information Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. The system requires a command line confirmation before the command executes. This command clears the following counters:

- hello Rx and Tx counters
- Topology change Rx and Tx counters
- The number of state change counters

Example (Summary)

```
Dell# show frrp summary
Ring-ID State Mode  Ctrl_Vlan Member_Vlans
-----------------------------------------------
2       UP   Master   2        11-20, 25,27-30
31      UP   Transit  31       40-41
50      Down Transit  50       32
Dell#
```

Example (1)

```
Dell# show frrp 1
Ring protocol 1 is in Master mode
Ring Protocol Interface:
Primary : TenGigabitEthernet 0/16 State: Forwarding
Secondary: Port-channel 100 State: Blocking
Control Vlan: 1
Ring protocol Timers: Hello-Interval 50 msec Dead-Interval 150 msec
Ring Master's MAC Address is 00:01:e8:13:a3:19
Topology Change Statistics: Tx:110 Rx:45
Hello Statistics: Tx:13028 Rx:12348
Number of state Changes: 34
Member Vlans: 1000-1009
Dell#
```

Example (2 Summary)

```
Dell# show frrp 2 summary
```

```
Dell# show frrp 2 summary
Ring-ID State Mode  Ctrl_Vlan Member_Vlans
-----------------------------------------------
2       Up    Master 2        11-20, 25, 27-30
Dell#
```

Related Commands protocol frrp — enters the resilient ring protocol and designate a ring identification.

timer

Set the hello interval or dead interval for the Ring control packets.

C9000 Series

Syntax `timer {hello-interval` *`milliseconds`*`}| {dead-interval` *`milliseconds`*`}`

To remove the timer, use the `no timer {hello-interval [milliseconds]}| {dead-interval milliseconds}` command.

Parameters

hello-interval *milliseconds*	Enter the keyword `hello-interval` then the time, in milliseconds, to set the hello interval of the control packets. The milliseconds must be entered in increments of 50 millisecond; for example, 50, 100, 150, and so on. If an invalid value is entered, an error message is generated. The range is from 50 to 2000 ms. Default: **500 ms**.
dead-interval *milliseconds*	Enter the keyword `dead-interval` then the time, in milliseconds, to set the dead interval of the control packets. The range is from 50 to 6000 ms. Default: **1500 ms**.

NOTE: The configured dead interval must be at least three times the hello interval.

Defaults

- **500 ms** for `hello-interval` *milliseconds*
- **1500 ms** for `dead-interval`*milliseconds*

Command Modes CONFIGURATION (conf-frrp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

Usage Information The `hello interval` command is the interval at which ring frames are generated from the primary interface of the master node. The `dead interval` command is the time that elapses before a time-out occurs.

19

GARP VLAN Registration (GVRP)

The Dell Networking OS supports basic GVRP commands on the switch.

The generic attribute registration protocol (GARP) mechanism allows the configuration of a GARP participant to propagate through a network quickly. A GARP participant registers or de-registers its attributes with other participants by making or withdrawing declarations of attributes. At the same time, based on received declarations or withdrawals, GARP handles attributes of other participants.

GVRP enables a device to propagate local VLAN registration information to other participant devices and dynamically update the VLAN registration information from other devices. The registration information updates local databases regarding active VLAN members and through which port the VLANs can be reached.

GVRP ensures that all participants on a bridged LAN maintain the same VLAN registration information. The VLAN registration information propagated by GVRP includes both manually configured local static entries and dynamic entries from other devices.

GVRP participants have the following components:

- The GVRP application
- GARP information propagation (GIP)
- GARP information declaration (GID)

Important Points to Remember

- GVRP is supported on Layer 2 ports only.
- All VLAN ports added by GVRP are tagged.
- GVRP is supported on untagged ports belonging to a default VLAN and tagged ports.
- GVRP cannot be enabled on untagged ports belonging to a non-default VLAN *unless* native VLAN is turned on.
- GVRP requires end stations with dynamic access NICs.
- Based on updates from GVRP-enabled devices, GVRP allows the system to dynamically create a port-based VLAN (unspecified) with a specific VLAN ID and a specific port.
- On a port-by-port basis, GVRP allows the system to learn about GVRP updates to an existing port-based VLAN with that VLAN ID and IEEE 802.1Q tagging.
- GVRP allows the system to send dynamic GVRP updates about your existing port-based VLAN.
- GVRP updates are not sent to any blocked spanning tree protocol (STP) ports. GVRP operates only on ports that are in the forwarding state.
- GVRP operates only on ports that are in the STP forwarding state. If you enable GVRP, a port that changes to the STP Forwarding state automatically begin to participate in GVRP. A port that changes to an STP state other than forwarding no longer participates in GVRP.
- VLANs created dynamically with GVRP exist only as long as a GVRP-enabled device is sending updates. If the devices no longer send updates, or GVRP is disabled, or the system is rebooted, all dynamic VLANs are removed.
- GVRP manages the active topology, not non-topological data such as VLAN protocols. If a local bridge must classify and analyze packets by VLAN protocols, manually configure protocol-based VLANs, and simply rely on GVRP for VLAN updates. But if the local bridge must know only how to reach a given VLAN, then GVRP provides all necessary information.
- The VLAN topologies that GVRP learns are treated differently from VLANs that are statically configured. The GVRP dynamic updates are not saved in NVRAM, while static updates are saved in NVRAM. When GVRP is disabled, the system deletes all VLAN interfaces that were learned through GVRP and leaves unchanged all VLANs that were manually configured.

Topics:

- clear gvrp statistics
- debug gvrp
- disable
- garp timers
- gvrp enable
- gvrp registration
- protocol gvrp
- show config
- show garp timers
- show gvrp
- show gvrp statistics

clear gvrp statistics

Clear GVRP statistics on an interface.

C9000 Series

Syntax `clear gvrp statistics interface` *interface*

Parameters

interface *interface* Enter the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Related Commands show gvrp statistics — displays the GVRP statistics.

debug gvrp

Enable debugging on GVRP.

C9000 Series

Syntax

`debug gvrp {config | events | pdu}`

To disable debugging, use the `no debug gvrp {config | events | pdu}` command.

Parameters

config	Enter the keyword `config` to enable debugging on the GVRP configuration.
event	Enter the keyword `event` to enable debugging on the JOIN/LEAVE events.
pdu	Enter the keyword `pdu` then one of the following Interface keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

Disabled.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

disable

Globally disable GVRP.

C9000 Series

Syntax

```
disable
```

To re-enable GVRP, use the `no disable` command.

Defaults Enabled.

Command Modes CONFIGURATION-GVRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Related Commands gvrp enable — enables GVRP on physical interfaces and LAGs.

protocol gvrp — access GVRP protocol.

garp timers

Set the intervals (in milliseconds) for sending GARP messages.

C9000 Series

Syntax

```
garp timers {join | leave | leave-all}
```

To return to the previous setting, use the `no garp timers {join | leave | leave-all}` command.

Parameters

join Enter the keyword `join` then the number of milliseconds to configure the join time. The range is from 100 to 147483647 milliseconds. The default is **200 milliseconds**.

NOTE: Designate the milliseconds in multiples of 100.

leave Enter the keyword `leave` then the number of milliseconds to configure the leave time. The range is from 100 to 2147483647 milliseconds. The default is **600 milliseconds**.

NOTE: Designate the milliseconds in multiples of 100.

leave-all Enter the keywords `leave-all` then the number of milliseconds to configure the leave-all time. The range is from 100 to 2147483647 milliseconds. The default is 1000 milliseconds.

NOTE: Designate the milliseconds in multiples of 100.

Defaults As above.

Command Modes CONFIGURATION-GVRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Usage Information

- Join Timer — `Join` messages announce the willingness to register some attributes with other participants. For reliability, each GARP application entity sends a `Join` message twice and uses a join timer to set the sending interval.
- Leave Timer — `Leave` announces the willingness to de-register with other participants. Together with `Join`, `Leave` messages help GARP participants complete attribute reregistration and de-registration. The leave timer starts after receipt of a leave message sent for de-registering some attribute information. If a `Join` message is *not* received before the `Leave` time expires, the GARP application entity removes the attribute information as requested.
- Leave All Timer — The `Leave All` timer starts when a GARP application entity starts. When this timer expires, the entity sends a `Leave-all` message so that other entities can reregister their attribute information. Then the `Leave-all` time begins again.

Related Commands show garp timers — displays the current GARP times.

gvrp enable

Enable GVRP on physical interfaces and LAGs.

C9000 Series

Syntax

`gvrp enable`

To disable GVRP on the interface, use the `no gvrp enable` command.

Defaults

Disabled.

Command Modes

CONFIGURATION-INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Related Commands

disable — globally disables GVRP.

gvrp registration

Configure the GVRP register type.

C9000 Series

Syntax

`gvrp registration {fixed | normal | forbidden}`

To return to the default, use the `gvrp register normal` command.

Parameters

fixed	Enter the keyword `fixed` then the VLAN range in a comma-separated VLAN ID set.
normal	Enter the keyword `normal` then the VLAN range in a comma-separated VLAN ID set. This setting is the default.
forbidden	Enter the keyword `forbidden` then the VLAN range in a comma-separated VLAN ID set.

Defaults **normal**

Command Modes CONFIGURATION-INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Usage Information Fixed registration prevents an interface, configured using the command line, to belong to a VLAN (static configuration) from being unconfigured when it receives a `Leave` message. Therefore, Registration mode on that interface is fixed.

Normal registration is the default registration. The port's membership in the VLAN depends on GVRP. The interface becomes a member of a VLAN after learning about the VLAN through GVRP. If the VLAN is removed from the port that sends GVRP advertisements to this device, the port stops being a member of the VLAN.

To advertise or learn about VLANs through GVRP, use the `forbidden` command when you do not want the interface.

Related Commands show gvrp — displays the GVRP configuration including the registration.

protocol gvrp

Access GVRP protocol — (config-gvrp)#.

C9000 Series

Syntax `protocol gvrp`

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Related Commands disable — globally disables GVRP.

show config

Display the global GVRP configuration.

C9000 Series

Syntax `show config`

Command Modes CONFIGURATION-GVRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Related Commands gvrp enable — enables GVRP on physical interfaces and LAGs.

protocol gvrp — accesses the GVRP protocol.

show garp timers

Display the GARP timer settings for sending GARP messages.

C9000 Series

Syntax `show garp timers`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Example

```
Dell# show garp timers
GARP Timers      Value (milliseconds)
----------------------------------------
Join Timer         200
Leave Timer        600
LeaveAll Timer     10000
Dell#
```

Related Commands garp timers — sets the intervals (in milliseconds) for sending GARP messages.

show gvrp

Display the GVRP configuration.

C9000 Series

Syntax `show gvrp [brief | interface]`

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to display a brief summary of the GVRP configuration.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Usage Information If no ports are GVRP participants, the message output changes from `GVRP Participants running on <port_list>` to `GVRP Participants running on no ports`.

Example

```
R3# show gvrp brief
GVRP Feature is currently enabled.
Port                GVRP Status      Edge-Port
-----------------------------------------------
Te 1/0              Disabled          No
Te 1/1              Disabled          No
Te 1/2              Enabled           No
Te 1/3              Disabled          No
Te 1/4              Disabled          No
Te 1/5              Disabled          No
Te 1/6              Disabled          No
Te 1/7              Disabled          No
Te 1/8              Disabled          No
R3# show gvrp brief
```

Related Commands show gvrp statistics — displays the GVRP statistics.

show gvrp statistics

Display the GVRP configuration statistics.

C9000 Series

Syntax

```
show gvrp statistics {interface interface | summary}
```

Parameters

interface *interface*	(OPTIONAL) Enter the keyword `interface` then one of the interface keywords and slot/ port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information.
summary	Enter the keyword `summary` to display just a summary of the GVRP statistics.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Inroduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on C-Series, E-Series, and S-Series

Usage Information

Invalid messages/attributes skipped can occur in the following cases:

- The incoming GVRP PDU has an incorrect length.
- "End of PDU" was reached before the complete attribute could be parsed.
- The Attribute Type of the attribute that was being parsed was not the GVRP VID Attribute Type (0x01).
- The attribute that was being parsed had an invalid attribute length.
- The attribute that was being parsed had an invalid GARP event.
- The attribute that was being parsed had an invalid VLAN ID. The valid range is from 1 to 4095.

A failed registration can occur for the following reasons:

- `Join` requests were received on a port that was blocked from learning dynamic VLANs (GVRP Blocking state).

- An entry for a new GVRP VLAN could not be created in the GVRP database.

Example

```
Dell# show gvrp statistics int te 1/0

Join Empty Received: 0
Join In Received: 0
Empty Received: 0
LeaveIn Received: 0
Leave Empty Received: 0
Leave All Received: 40
Join Empty Transmitted: 156
Join In Transmitted: 0
Empty Transmitted: 0
Leave In Transmitted: 0
Leave Empty Transmitted: 0
Leave All Transmitted: 41
Invalid Messages/Attributes skipped: 0
Failed Registrations: 0
Dell#
```

Related Commands show gvrp — displays the GVRP configuration.

20

High Availability (HA)

High availability (HA) in the Dell Networking operating software is configuration synchronization to minimize recovery time in the event of a route processor module (RPM) failure.

In general, a protocol is defined as "hitless" in the context of an RPM failure/failover and not failures of a line card, SFM, or power module. A protocol is defined as hitless if an RPM failover has no impact on the protocol.

You must specifically enable some protocols for HA. Some protocols are only hitless if related protocols are also enabled as hitless (for example, the `redundancy protocol` command).

Topics:

- redundancy auto-failover-limit
- redundancy disable-auto-reboot
- redundancy force-failover
- redundancy primary
- redundancy reset-counter
- redundancy synchronize
- show redundancy

redundancy auto-failover-limit

Specify an auto-failover limit for RPMs and PEs. When a non-recoverable fatal error is detected, an automatic RPM or PE failover occurs. This command does not affect user-initiated (manual) failovers.

C9000 Series

Syntax

`redundancy auto-failover-limit [count` *`number`* `[period` *`minutes`*`] | period` *`minutes`*`]]`

To disable the auto-failover limit control, use the `no redundancy auto-failover-limit` command.

Parameters

count *number*	Enter the number of times the RPMs or PEs can automatically failover within the period defined in the period parameter. The range is from 2 to 10. The default is **3**.
period *minutes*	Enter a duration in which to allow a number of automatic failovers (limited to the number defined in the count parameter). The range is from 5 to 9000 minutes. The default is **60 minutes**.

Default

- Count: **3**
- Period: **60 minutes**

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series

Usage Information

If you disable auto failover, enter the `redundancy auto-failover-limit` (without any parameters) to set auto failover to the default parameters (Count 3, Period 60 minutes). To view the redundancy status, use the `show redundancy` command.

When you change one or both of the optional parameters, Dell Networking OS checks that the interval between auto failovers is more than five (5) minutes. If the interval is less, Dell Networking OS returns a configuration error message.

redundancy disable-auto-reboot

Prevent the system from auto-rebooting the failed module.

C9000 Series

Syntax

`redundancy disable-auto-reboot {linecard [slot—id | all] | pe` *`pe-id`* `stack unit` *`unit-number`* `| all | rpm}`

Parameters

lincard *slot-id* / all	Enter the keyword `linecard` with the *slot-id* to specify a linecard, or `all` to select all linecards. Linecard ID. Range is from 0 to 11.
pe *pe-id* / all	Enter the keyword `pe` and the port extender ID or type the option `all` to select all port extenders. Range is from 0 to 255.
stack unit *unit-number*	Enter the keyword `stack-unit` and the configuration is applied to all the stack-units present in the PE.
rpm	Enter the keyword `rpm` to disable auto-reboot of the failed RPM.

Default

Disabled (that is, the failed module is automatically rebooted).

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the `all` option.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the E-Series

Usage Information Enabling this command keeps the failed module (RPM, PE, or Linecard) in the failed state. If there are two RPMs or PEs in the system, enabling this command prevents the failed RPM or PE from becoming a working Standby RPM or PE. If there is only one RPM or PE in the system, the failed RPM or PE does not recover and affects the system.

Example: PE

```
Dell(conf)#redundancy disable-auto-reboot pe 1 stack-unit
```

redundancy force-failover

Force the standby unit to become the primary or master unit. You can also use this command to upgrade the software on one unit from the other when the other has been loaded with the upgraded software.

C9000 Series

Syntax

```
redundancy force-failover { rpm | pe pe-id }
```

Parameters

rpm	Enter the keyword `rpm` to force the standby RPM to become the primary RPM.
pe *pe-id*	Enter the keyword `pe` and the port extender ID to force the standby stack unit to become the primary (or master) stack unit. Range is from 0 to 255.

Default Not configured.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command-Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

The `redundancy force-failover pe` command forces a standby port extender unit to become a primary (or master) unit.

Example

```
Dell#redundancy force-failover pe 255
```

Related Commands

stack-unit — Pre-provision the specified port-extender stack unit.

redundancy primary

Set an RPM as the primary RPM.

C9000 Series

Syntax

`redundancy primary [rpm0 | rpm1]`

To delete a configuration, use the `no redundancy primary` command.

Parameters

rpm0	Enter the keyword `rpm0` to set the RPM in slot R0 as the primary RPM.
rpm1	Enter the keyword `rpm1` to set the RPM in slot R1 as the primary RPM.

Default

The RPM in slot R0 is the Primary RPM.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

redundancy reset-counter

Reset failover counter and timestamp information displayed in the `show redundancy` command output.

C9000 Series

Syntax `redundancy reset-counter pe pe-id`

Parameters

pe *pe-id*	Enter the keyword `pe` and the port extender ID to reset the counter. Range is from 0 to 255.

Default Not configured.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the E-Series.

Example

```
Dell#redundancy reset-counter pe 1
```

redundancy synchronize

Manually synchronize data between the RPMs and PEs at any time.

C9000 Series

Syntax `redundancy synchronize [full]`

Parameters

full	Enter the keyword `full` to synchronize all data.

Default Not configured.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Data between the two RPMs or PEs is synchronized immediately after bootup. Once the two RPMs or PEs complete an initial full synchronization (block sync), the Dell Networking OS updates changed data (incremental sync).The data that is synchronized consists of configuration data, operational data, state and status, and statistics depending on the Dell Networking OS version.

show redundancy

Display the current redundancy configuration.

C9000 Series

Syntax

`show redundancy pe` *`pe-id`*

From a **PE console**, use `show redundancy` to view the current high availability (HA) status for a specified port extender unit.

Parameters

pe *pe-id*	Enter the keyword `pe` and the port extender ID to display the current redundancy configuration of the specified port extender unit. Range is from 0 to 255

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.

Version	Description
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

To modify your results, use the `show redundancy [pipe]` command, as follows:

- `except` — show only text that doesn not match a pattern.
- `find` — search for the first occurrence of a pattern.
- `grep` — show only text that matches a pattern.
- `no-more` — do not paginate the output.
- `save` — save the output to a file.

The following describes the `show redundancy` command shown in the following example.

Field	Description
RPM Status	Displays the following information: • Slot number of the RPM. • Whether the RPM is Primary or Standby. • The state of the RPM: Active, Standby, Booting, or Offline. • Whether the link to the second RPM is up or down.
PEER RPM Status	Displays the state of the second RPM, if present
RPM Redundancy Configuration	Displays the following information: • which RPM is the preferred Primary on next boot (the `redundancy primary` command) • the data sync method configured (the `redundancy synchronize` command) • the failover type (you cannot change this type; it is software-dependent). **Hot Failover** means that the running configuration and routing table are applied on secondary RPM. **Fast Failover** means that the running configuration is not applied on the secondary RPM until failover occurs, and the routing table on line cards is cleared during failover. • the status of auto booting the RPM (the `redundancy disable-auto-reboot` command) • the parameter for auto failover limit control (the `redundancy auto-failover-limit` command)
RPM Failover Record	Displays the following information: • RPM failover counter (to reset the counter, use the `redundancy reset-counter` command) • the time and date of the last RPM failover

Field	Description
	• the reason for the last RPM failover
Last Data Sync Record	Displays the data sync information and the timestamp for the data sync: • Start-up Config is the contents of the startup-config file. • Line Card Config is the line card types configured and interfaces on those line cards. • Runtime Event Log is the contents of the Event log. • Running Config is the current running-config. This field only appears when you enter the command from the Primary RPM.

Example

```
Dell# show redundancy

-- RPM Status --
-----------------------------------------------
RPM Slot ID:         1
RPM Redundancy Role: Primary
RPM State:           Active
RPM SW Version:      7.5.1.0
Link to Peer:        Up

-- PEER RPM Status --
-----------------------------------------------
RPM State:       Standby
RPM SW Version:  7.5.1.0

-- RPM Redundancy Configuration --
-----------------------------------------------
Primary RPM:         rpm0
Auto Data Sync:      Full
Failover Type:       Hot Failover
Auto reboot RPM:     Enabled
Auto failover limit: 3 times in 60 minutes

-- RPM Failover Record --
-----------------------------------------------
Failover Count:           1
Last failover timestamp:  Jul 13 2007 21:25:32
Last failover Reason:     User request

-- Last Data Block Sync Record: --
-----------------------------------------------
Line Card Config:  succeeded Jul 13 2007 21:28:53
Start-up Config:   succeeded Jul 13 2007 21:28:53
SFM Config State:  succeeded Jul 13 2007 21:28:53
Runtime Event Log: succeeded Jul 13 2007 21:28:53
Running Config:    succeeded Jul 13 2007 21:28:53
Dell#
```

Example: show redundancy pe *pe-id*

```
Dell#show redundancy pe 0

--  pe Status  --
-----------------------------------------------
Mgmt ID:                          0
pe ID:                            0
pe Redundancy Role:               Primary
pe State:                         Active
pe SW Version:                    1-0(0-4098)
Link to Peer:                     Up

--  PEER pe Status  --
-----------------------------------------------
```

```
pe State:                          Standby
Peer pe stack unit ID:             2
pe SW Version:                     1-0(0-4098)

--  pe Redundancy Configuration  --
-----------------------------------------------
Primary pe:                        mgmt-id    0
Auto Data Sync:                    Full
Failover Type:                     Hot Failover
Auto reboot pe:                    Disabled
Auto failover limit:               3 times in 60 minutes

--  pe Failover Record  --
-----------------------------------------------
Failover Count:                    0
Last failover timestamp:           None
Last failover Reason:              None
Last failover type:                None

--  Last Data Block Sync Record:  --
-----------------------------------------------
stack-unit Config:          succeeded  Jun 26 2015 16:39:41
Runtime Event Log:          succeeded  Jun 26 2015 16:39:41
    Running Config:          succeeded  Jun 26 2015 16:39:41
```

21

ICMP Message Types

This section lists and describes the possible ICMP message type resulting from a ping. The first three columns list the possible symbol or type/code. For example, you would receive a ! or 03 as an echo reply from your ping.

Table 3. ICMP messages and their definitions

Symbol	Type	Code	Description	Query	Error
.			Timeout (no reply)		
!	0	3	echo reply	.	
U	3		destination unreachable:		
		0	network unreachable		.
		1	host unreachable		.
		2	protocol unreachable		.
		3	port unreachable		.
		4	fragmentation needed but don't fragment bit set		.
		5	source route failed		.
		6	destination network unknown		.
		7	destination host unknown		.
		8	source host isolated (obsolete)		.
		9	destination network administratively prohibited		.
		10	destination host administratively prohibited		.
		11	network unreachable for TOS		.
		12	host unreachable for TOS		.
		13	communication administratively prohibited by filtering		.
		14	host precedence violation		.
		15	precedence cutoff in effect		.
C	4	0	source quench		.
	5		redirect		.
		0	redirect for network		.
		1	redirect for host		.
		2	redirect for type-of-service and network		.
		3	redirect for type-of-service and host		.
	8	0	echo request	.	
	9	0	router advertisement	.	
	10	0	router solicitation	.	

Symbol	Type	Code	Description	Query	Error
&	11		time exceeded:		
		0	time-to-live equals 0 during transit		.
		1	time-to-live equals 0 during reassembly		.
	12		parameter problem:		
		1	IP header bad (catchall error)		.
		2	required option missing		.
	13	0	timestamp request	.	
	14	0	timestamp reply	.	
	15	0	information request (obsolete)	.	
	16	0	information reply (obsolete)	.	
	17	0	address mask request	.	
	18	0	address mask reply	.	

22

Interfaces

The Dell Networking OS supports the interface configuration commands described in this chapter.

This chapter contains the following sections:

- Basic Interface Commands
- EIS Commands
- Port Channel Commands
- High-Gigabit Port Channel Commands

Topics:

- Basic Interface Commands
- Egress Interface Selection (EIS) Commands
- Port Channel Commands
- HiGig Port Channel Commands
- Time Domain Reflectometer (TDR) Commands

Basic Interface Commands

The following commands are for Physical, Loopback, and Null interfaces.

clear counters

Clear the counters used in the show interfaces commands for all virtual router redundancy protocol (VRRP) groups, virtual local area networks (VLANs), and physical interfaces, or selected ones.

C9000 Series

Syntax `clear counters [interface] [vrrp [ipv6 {vrid} | learning-limit | vlan vlan-id]`

Parameters

interface (OPTIONAL) Enter any of the following keywords and slot/port, *pe-id/stack-unit/port* or number to clear counters from a specified interface:

- For IPv4 access-group counters, enter the keyword `ip`.
- For IPv6 access-group counters, enter the keyword `ipv6`.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For MAC access-group counters, enter the keyword `mac`.
- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* (ports, port-range) information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096.

- For the management interface on the RPM, enter the keyword `ManagementEthernet` then slot/port information. The slot range is from 0 to 1 and the port range is 0.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port (ports, port-range) information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port (range of ports) information.
- For a tunnel interface, enter the keyword `tunnel`. The range is from 1 to 16383.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

vrrp [[ipv6] *vrid*] (OPTIONAL) Enter the keyword `vrrp` to clear the counters of all VRRP groups. To clear the counters of VRRP groups on all IPv6 interfaces, enter `ipv6`. To clear the counters of a specified group, enter a VRID number from 1 to 255.

learning-limit (OPTIONAL) Enter the keywords `learning-limit` to clear unknown source address (SA) drop counters when MAC learning limit is configured on the interface.

vlan *vlan-id* Enter the keyword `vlan` then the interface VLAN number. The range is from 1 to 4094.

Defaults

Without an interface specified, the command clears all interface counters.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Added the `vlan` parameter.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.4.1.0	Added support (E-Series only) for VRRP groups in a VRF instance.
8.3.7.0	Introduced on the S4810.

Version	Description
8.2.1.0	Added support for 4093 VLANs on the E-Series ExaScale. Prior to the release, 2094 was supported.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Updated the definition of the `learning-limit` option for clarity.

Usage Information

To clear counters for multiple ports on the interfaces at one time. You can specify any random port number or a range of ports, or a combination of both.

To clear counters for a range of ports, you can enter a hyphenated range of one or more port range values separated with commas; for example, `clear counters FortyGigE 1/0-4,7,9-11`. To clear counters for any random number of ports, you can enter a comma-separated string of port numbers, for example `clear counters FortyGigE 1/0/1,9,11`

In a dual homing setup, you can use this command only from the primary VLT peer.

You can use the `vlan`, `learning-limit`, and `vrrp` keyword options for multiple ports.

NOTE: The port-range option is only available for 1 Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, Port Channel, and VLAN interfaces.

Example

```
Dell#clear counters
Clear counters on all interfaces [confirm] yes
```

Clear counters for a range of ports

```
Dell#clear counters fortyGigE 0/0-12
Clear counters on Fo 0/0-12
Clear counters on Fo 0/0-12 [confirm] yes
```

Clear counters for any random port number

```
Dell#clear counters fortyGigE 0/0,28
Clear counters on Fo 0/0,28
Clear counters on Fo 0/0,28 [confirm] yes
```

Example (learning-limit)

Clear learning-limit counters for a single port

```
Dell#clear counters tengigabitethernet 0/8 learning-limit
Clear "show learning-limit" counters on Te 0/8 [confirm] y
```

Clear learning-limit counters for a range of ports

```
Dell#clear counters tengigabitethernet 0/8-12 learning-limit
Clear "show learning-limit" counters on Te 0/8-12 [confirm] y
```

Clear learning-limit counters for any random port number

```
Dell#clear counters tengigabitethernet 0/8,16 learning-limit
Clear "show learning-limit" counters on Te 0/8,16 [confirm] y
```

Example (vrrp-multiple-ports)

```
Clear vrrp counters for a single port
Dell# clear counters fortyGigE 0/8 vrrp 3
Clear "show vrrp" counters of IPv4 vrrp group (3) on Fo 0/8 [confirm] y
```

```
Clear vrrp counters for a range of ports
Dell#clear counters fortyGigE 0/8-12 vrrp 3
Clear "show vrrp" counters of IPv4 vrrp group (3) on Fo 0/8-12 [confirm] y
```

```
Clear vrrp counters for any random port number
Dell#clear counters fortyGigE 0/8,16 vrrp 3
Clear "show vrrp" counters of IPv4 vrrp group (3) on Fo 0/8,16  [confirm] y
```

Example (vlan-multiple-ports)

```
Dell#clear counters vlan 1,13
Clear counters on Vl 1, 13 [confirm] yes
```

Related Commands

- mac learning-limit — allows aging of MACs even though a learning-limit is configured or disallow station move on learned MACs.
- show interfaces — displays information on the interfaces.

clear dampening

Clear the dampening counters on all the interfaces or just the specified interface.

C9000 Series

Syntax

```
clear dampening [interface]
```

Parameters

interface (OPTIONAL) Enter any of the following keywords and slot/port or number to clear counters from a specified interface:

- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 0 to 47.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit `unit-number` range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults Without an interface specified, the command clears all interface dampening counters.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell# clear dampening tengigabitethernet 1/2
Clear dampening counters on Te 1/2 [confirm] y
Dell#
```

Related Commands

- show interfaces dampening — displays interface dampening information.
- dampening — configures dampening on an interface.

combo-port-type

You can pre-provision the medium of combo ports as copper or fiber.

Syntax `combo-port-type{copper | fiber}`

Parameters

copper	Enter the keyword `copper` to provision the combo port as a copper port.
fiber	Enter the keyword `fiber` to provision the combo port as a fiber port.

Defaults None

Command Modes INTERFACE

Command History

Version	Description
9.11(0.0)	Introduced on the N20xx and N30xx series port extenders.
9.10(0.0)	Introduced on the S3100 series.

Usage Information By default, a combo port is in Hybrid mode. Use the `combo-port-type` command to provision the combo port as either copper or fiber. Use the `no combo-port-type` command to change the combo port to Hybrid mode.

The `negotiation auto` command is not available on the combo ports in the hybrid mode. You need to provision the combo port as copper or fiber medium using the `combo-port-type` command.

Example

```
Dell(conf-if-pegi-2/0/48)# combo-port-type copper
Dell(conf-if-pegi-2/0/48)# combo-port-type fiber
```

combo-port-type

You can pre-provision the medium of combo ports as copper or fiber.

Syntax `combo-port-type{copper | fiber}`

Parameters

copper	Enter the keyword `copper` to provision the combo port as a copper port.
fiber	Enter the keyword `fiber` to provision the combo port as a fiber port.

Defaults None

Command Modes INTERFACE

Command History

Version	Description
9.11(0.0)	Introduced on the N20xx and N30xx series port extenders.
9.10(0.0)	Introduced on the S3100 series.

Usage Information

By default, a combo port is in Hybrid mode. Use the `combo-port-type` command to provision the combo port as either copper or fiber. Use the `no combo-port-type` command to change the combo port to Hybrid mode.

The `negotiation auto` command is not available on the combo ports in the hybrid mode. You need to provision the combo port as copper or fiber medium using the `combo-port-type` command.

Example

```
Dell(conf-if-pegi-2/0/48)# combo-port-type copper
Dell(conf-if-pegi-2/0/48)# combo-port-type fiber
```

dampening

Configure dampening on an interface.

C9000 Series

Syntax `dampening [[[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]`

Parameters

half-life	Enter the number of seconds after which the penalty is decreased. The penalty decreases half after the half-life period expires. The range is from 1 to 30 seconds. The default is **5 seconds**.
reuse-threshold	Enter a number as the reuse threshold, the penalty value below which the interface state is changed to "up". The range is from 1 to 20000. The default is **750**.

suppress-threshold	Enter a number as the suppress threshold, the penalty value above which the interface state is changed to "error disabled". The range is from 1 to 20000. The default is **2500**.
max-suppress-time	Enter the maximum number for which a route can be suppressed. The default is four times the half-life value. The range is from 1 to 86400. The default is **20 seconds**.

Defaults Disabled.

Command Modes INTERFACE (conf-if-)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information With each flap, the system penalizes the interface by assigning a penalty (1024) that decays exponentially depending on the configured half-life. After the accumulated penalty exceeds the suppress threshold value, the interface moves to the Error-Disabled state. This interface state is deemed as "down" by all static/dynamic Layer 2 and Layer 3 protocols. The penalty is exponentially decayed based on the half-life timer. After the penalty decays below the reuse threshold, the interface enables. The configured parameters are as follows:

- `suppress-threshold` should be greater than `reuse-threshold`
- `max-suppress-time` should be at least 4 times `half-life`

NOTE: You cannot apply dampening on an interface that is monitoring traffic for other interfaces.

Example

```
Dell(conf-if-te-2/2)# dampening 20 800 4500 120
Dell(conf-if-te-2/2)#
```

Related Commands

- clear dampening — clears the dampening counters on all the interfaces or just the specified interface.
- show interfaces dampening — displays interface dampening information.

description

Assign a descriptive text string to the interface.

C9000 Series

Syntax

`description desc_text`

To delete a description, use the `no description` command.

Parameters

desc_text	Enter a text string up to 240 characters long.

Defaults

none

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Modified for E-Series: Revised from 78 to 240 characters.

Usage Information

Important Points to Remember:

- To use special characters as a part of the description string, you must enclose the whole string in double quotes.
- Spaces between characters are not preserved after entering this command unless you enclose the entire description in quotation marks ("*desc_text*").
- Entering a text string after the `description` command overwrites any previous text string that you previously configured as the description.
- The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port-channel.
- Use the `show interfaces description` command to display descriptions configured for each interface.

Related Commands

show interfaces — displays information about an interface.

default interface

Resets a physical interface to its factory-default settings.

C9000 Series

Syntax

```
default interface interface slot/port-range
```

Parameters

interface slot/port-range	Enter one of the following interface types and port information to specify a single port or a range of ports. To specify a port range, you can enter a hyphenated range and/or individual port numbers separated with commas; for example, `default interface tengigabitethernet 1/0-4,7,9-11`. To enter any random number of ports, you can enter a comma-separated string of port numbers, for example `default interface tengigabitethernet 1/0,1,9,11` • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010, FNXML, MXL, S4810, S4820T, S3048-ON, S4048-ON, S5000, S6000, S6000-ON, and Z9500.

Usage Information

Use the `default interface` command to set a 10-Gigabit Ethernet or 40-Gigabit Ethernet interface to its factory-default state. By default, a physical interface is disabled (`shutdown`) with no assigned IP address or switchport (`no ip address`).

This command removes all software settings and all L3, VLAN, VXLAN, and port-channel configurations on a physical interface.

Example

```
Dell# show running-config interface tengigabitethernet 0/30
!
interface TenGigabitEthernet 0/30
 no ip address
 switchport
 switchport mode private-vlan host
 rate-interval 8
 mac learning-limit 10 no-station-move
 shutdown

Dell#show running-config interface vlan 33
!
interface Vlan 33
```

```
 private-vlan mode isolated
 no ip address
 tagged TenGigabitEthernet 0/30
 shutdown

Dell(conf)# default interface tengigabitethernet 0/30
Dell# show running-config interface tengigabitethernet 0/30
!
interface TenGigabitEthernet 0/30
 no ip address
 shutdown

Dell#show running-config interface vlan 33
!
interface Vlan 33
 private-vlan mode isolated
 no ip address
shutdown
```

Related Commands show running-config— displays the current configuration.

encapsulation dot1q

Configures lite-subinterfaces.

Syntax `encapsulation dot1q vlan-id`

To remove a previously configured lite-subinterface, use the `no encapsulation dot1q vlan-id` command.

Parameters

dot1q *vlan-id*	Enter the keyword `dot1q` followed by the VLAN ID to which the host belongs. The range is from 1 to 4094. A lite subinterface is considered as a Layer 3 port property and is synchronous with the existing rules of applying Layer 2 or Layer 3 properties to an interface.

Command Modes INTERFACE

Command History

Version	Description
9.12.1.0	Introduced on the S5048F–ON.
9.10(0.1)	Introduced on the S6010-ON and S4048-ON.
9.10(0.0)	Introduced on the S6100–ON.
9.8(1.0)	Introduced on the Z9100–ON.
9.3.0.0	Introduced on the S6000.
9.2(1.0)	Introduced on the Z9500.

Usage Information To enable routing of RRoCE packets, the VLAN ID is mapped to the default VLAN ID of 4095 and this mapping is performed using VLAN translation. After VLAN translation, the RRoCE packets are considered in the same manner as normal IP packets that received on L3 interface and routed in the egress direction. At the egress interface, the VLAN ID is appended to the packet and transmitted out of the interface as a tagged packet with the dot1Q value preserved. The dot1Q value is preserved only for egress interfaces that are associated with a VLAN or a lite-subinterface . If a Layer 3 interface is configured without the encapsulation 802.1Q VLAN ID or is an untagged interface in a VLAN , the dot1Q value is not preserved .

flowcontrol

Enable and disable link-level flow control (802.3x pause frames) on an interface and (optionally) configure buffer thresholds for pause and offset frame transmission.

C9000 Series

Syntax

```
flowcontrol {rx {off | on} tx {off | on} [pause-threshold {1-12480}] | [resume-offset {1-12480}] | monitor session-ID
```

Parameters

rx on	Enter the keywords `rx on` to process the received flow control frames on this port.
rx off	Enter the keywords `rx off` to ignore the received flow control frames on this port.
tx on	Enter the keywords `tx on` to send control frames from the port to the connected device when a higher rate of traffic is received.
tx off	Enter the keywords `tx off` so that flow control frames are not sent from this port to the connected device when a higher rate of traffic is received.
pause-threshold	Enter the keyword `pause-threshold` to configure the buffer threshold (in Kilobytes) at which the interface starts transmitting pause frames for link-level flow control. Valid values are 1 to 12480KB. The default is 60KB.
resume-offset	Enter the keyword `resume-offset` to configure the buffer threshold (in Kilobytes) at which the interface resumes transmitting offset frames for link-level flow control. Valid values are 1 to 12480KB. The default is 9KB.
monitor	Enter the keyword `monitor` then the session-ID to enable mirror flow control frames on the interface. The range is from 0 to 65535.

Defaults

An interface ignores flow-control frames received from other network devices (**rx off**) and does not transmit pause frames (**tx off**).

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Added support for monitor session.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
6.5.1.9/7.4.1.0	Introduced on the E-Series.

Version	Description
7.8.1.0	Introduced on the C-Series and S-Series with the `thresholds` option.

Usage Information

The globally assigned 48-bit Multicast address 01-80-C2-00-00-01 is used to send and receive pause frames. To allow full-duplex flow control, stations implementing the pause operation instruct the MAC to enable the reception of frames with a destination address equal to this multicast address.

The pause:

- Starts when *either* the packet pointer or the buffer threshold is met (whichever is met first). When the discard threshold is met, packets are dropped.
- Ends when *both* the packet pointer and the buffer threshold fall below 50% of the threshold settings.

The *discard threshold* defines when the interface starts dropping the packet on the interface. This may be necessary when a connected device does not honor the flow control frame sent by the switch. The discard threshold should be larger than the *buffer threshold* so that the buffer holds at least hold at least three packets.

Changes in the flow-control values may not be reflected automatically in the `show interface` output. As a workaround, apply the new settings, execute `shut` then `no shut` on the interface, then check the running-config of the port using the `show interface` command.

Important Points to Remember

- Do not enable `tx pause` when buffer carving is enabled. For information and assistance, consult Dell Networking TAC.
- Asymmetric flow control (`rx on tx off`, or `rx off tx on`) setting for the interface port less than 100 Mb/s speed is not permitted. The following error is returned:
  `Can't configure Asymmetric flowcontrol when speed <1G, config ignored`
- The only configuration applicable to half duplex ports is `rx off tx off`. The following error is returned:
  `Can't configure flowcontrol when half duplex is configure, config ignored`
- Half duplex cannot be configured when the flow control configuration is on (default is `rx on tx on`). The following error is returned:
  `Can't configure half duplex when flowcontrol is on, config ignored`

NOTE: The flow control must be off (`rx off tx off`) before configuring the half duplex.

NOTE: If you use the `disable rx flow control` command, Dell Networking recommends rebooting the system.

NOTE: The flow control feature is not supported on the Port Extender Gigabit Ethernet (peGigE) interface.

Example

```
Dell(conf-if-te-0/1)# show config
!
interface TengigabitEthernet 0/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on monitor 9
no shutdown
...
```

Related Commands

- show running-config — displays the flow configuration parameters (non-default values only).
- show interfaces — displays the negotiated flow control parameters.

interface

Configure a physical or logical interfaces on the switch.

C9000 Series

Syntax `interface interface range [group interface]`

Parameters

interface Enter one of the following keywords and slot/port, *pe-id* /stack-unit or number information:

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information.
- For a Loopback interface, enter the keyword `loopback` then the slot/port information. The range is from 0 to 16383.
- For a Management Ethernet interface, enter the keyword `managementethernet` then the slot/port information.
- For a null interface, enter the keyword `null` then the slot/port information. The Null interface number is 0.
- For a Port Channel interface, enter the keyword `port-channel` then the port-channel ID. Range is from 1 to 4096.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a Tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.
- For a VLAN interface, enter the keyword `vlan` then the slot/port information. The range is from 1 to 4094.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

group *interface* (Optional) Enter the keyword `group` to configure an interface group. You can create a interface group by adding a comma or hyphen separate list of the following interface types:

- `fortyGigE` for a 40–Gigabit Ethernet interface.
- `gigabitethernet` for a GigabitEthernet interface.
- `peGigE` for a PE Gigabit Ethernet interface.
- `peTenGigE` for a PE 10–Gigabit Ethernet interface.
- `TengigabitEthernet` for a 10-Gigabit Ethernet interface.
- `vlan` for a VLAN interface.

range (Optional) Enter the keyword `range` to configure an interface range.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Introduced

Usage Information You cannot delete a physical interface.

By default, physical interfaces are disabled (`shutdown`) and are not assigned to an IP address or switchport. To place an interface in Layer 2 mode, ensure that the interface's configuration does not contain an IP address and enter the `switchport` command.

You can create up to 64 tunnel interfaces. The tunnel is added as a logical interface with no default configuration. To delete a tunnel interface, use the `no interface tunnel` *`tunnel-id`* command.

Example

```
Dell(conf)# int tengigabitethernet 0/0
Dell(conf-if-te-0/0)#exit
Dell(conf)#
```

Example peGigE

```
Dell#show interfaces peGigE 0/0/0
peGigE 0/0/1 is up, line protocol is up
Hardware is DellEth, address is a0:68:00:3f:92:bd
    Current address is a0:68:00:3f:92:bd
Pluggable media not present
Interface index is 536870919
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :a068003f92bd
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex
Auto-mdix enabled, ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 02:44:11
Queueing strategy: fifo
Input Statistics:
     5150004 packets, 4996095648 bytes
     164432 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
```

```
     0 over 255-byte pkts, 4985572 over 511-byte pkts, 0 over 1023-byte pkts
     0 Multicasts, 0 Broadcasts, 5150004 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     11165065 packets, 714564160 bytes, 0 underruns
     11165065 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
     309 Multicasts, 0 Broadcasts, 11164756 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 140.00 Mbits/sec,      18070 packets/sec, 14.30% of line-rate
     Output 20.00 Mbits/sec,      39175 packets/sec, 2.60% of line-rate
Time since last interface status change: 02:37:06
```

Related Commands show interfaces — displays the interface configuration.

interface loopback

Configure a Loopback interface.

C9000 Series

Syntax `interface loopback number`

To remove a loopback interface, use the `no interface loopback number` command.

Parameters

number	Enter a number as the interface number. The range is from 0 to 16383.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Introduced

Example

```
Dell(conf)# interface loopback 1655
Dell(conf-if-lo-1655)#
```

Related Commands

interface — configures a physical interface.

interface null — configures a Null interface.

interface port-channel — configures a port channel.

interface vlan — configures a VLAN.

interface ManagementEthernet

Configure the Management port on the system (either the Primary or Standby RPM).

C9000 Series

Syntax

```
interface ManagementEthernet slot/port
```

Parameters

slot/port	Enter the keyword `ManagementEthernet`, then the slot number (0 or 1) and port number zero (0).

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.11.1	Introduced on the S55, S60, and S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Introduced

Usage Information

You cannot delete a Management port.

The Management port is enabled by default (`no shutdown`). To assign an IP address to the Management port, use the `ip address` command.

If your system has two RPMs installed, use the `show redundancy` command to display which RPM is the Primary RPM.

Example

```
Dell(conf)# interface managementethernet 0/0
Dell(conf-if-ma-0/0)#
```

Related Commands

management route — configures a static route that points to the Management interface or a forwarding router.

speed (Management interface) — clears the FIB entries on a specified line card.

interface null

Configure a Null interface on the switch.

C9000 Series

Syntax `interface null number`

Parameters

number	Enter zero (0) as the Null interface number.

Defaults Not configured; number = **0**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Introduced

Usage Information You cannot delete the Null interface. The only configuration command possible in a Null interface is `ip unreachables`.

Example

```
Dell(conf)# interface null 0
Dell(conf-if-nu-0)#
```

Related Commands

- interface — configures a physical interface.
- interface loopback — configures a Loopback interface.
- interface port-channel — configures a port channel.
- interface vlan — configures a VLAN.
- ip unreachables — enables generation of internet control message protocol (ICMP) unreachable messages.

interface range

This command permits configuration of a range of interfaces to which subsequent commands are applied (bulk configuration). Using the `interface range` command, you can enter identical commands for a range of interface.

C9000 Series

Syntax `interface range interface, interface,...`

Parameters

interface, interface,... Enter the keywords `interface range` and one of the interfaces — slot/port, port-channel, or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels, and physical interfaces.

Slot/Port information must contain a space before and after the dash. For example, `interface range tengigabitethernet 0/1 - 5` is valid; `interface range tengigabitethernet 0/1-5` is NOT valid.

- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a Tunnel interface, enter the keyword `Tunnel` then a number from 1 to 16383.
- For a Port Extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.14(0.0)	Updated the error message when no VLANs are configured within the specified interface range.
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Added support for 4093 VLANs on E-Series ExaScale. Prior releases supported 2094.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

When creating an interface range, interfaces appear in the order they are entered; they are not sorted. The command verifies that interfaces are present (physical) or configured (logical).

Important Points to Remember:

- Bulk configuration is created if at least one interface is valid.
- Non-existing interfaces are excluded from the bulk configuration with a warning message.
- The `interface range` prompt includes interface types with slot/port information for valid interfaces. The prompt allows for a maximum of 32 characters. If the bulk configuration exceeds 32 characters, it is represented by an ellipsis (...).
- For PE ports, the `interface range` prompt includes interface type with *pe-id / stack-unit / port-id*.
- When the `interface range` prompt has multiple port ranges, the smaller port range is excluded from the prompt.
- If overlapping port ranges are specified, the port range is extended to the smallest start port and the biggest end port.

Example (Bulk)

```
Dell EMC(conf)# interface range te 10/0, fo 0/0, te 2/0
% Warning: Non-existing ports (not configured) are ignored by
interface-range
```

Example (Multiple Ports)

```
Dell EMC(conf)# interface range te 2/0 - 23, te 2/1 - 10
Dell(conf-if-range-te-2/0-23#
```

Example (Overlapping Ports)

```
Dell EMC(conf)# interface range te 2/1 - 11, te 2/1 - 23
Dell(conf-if-range-te-2/1-23#
```

Example (If atleast one port is configured)

```
DellEMC(conf)# interface range tengigbitethernet 2/1 - 11, tengigbitethernet
2/1 - 23
% Warning: Non-existing ports (not configured) are ignored by
interface-range
```

Example (If no ports are configured within the specified interface range)

```
DellEMC(conf)# interface range tengigbitethernet 2/0 - 23, fortyGigE 0/0,
tengigbitethernet 2/0
% Error: No port is configured in interface range
```

Usage Information

Only VLAN and port-channel interfaces created using the `interface vlan` and `interface port-channel` commands can be used in the `interface range` command.

Use the `show running-config` command to display the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the `show running-config` command cannot be used with the bulk configuration feature of the `interface range` command. You cannot create virtual interfaces (VLAN, Port-channel) using the `interface range` command.

NOTE: If a range has VLAN, physical, and port-channel interfaces, only commands related to physical interfaces can be bulk configured. To configure commands specific to VLAN or port-channel, only those respective interfaces should be configured in a particular range.

Example (Single Range)

This example shows a single range bulk configuration.

```
Dell(config)# interface range tengigabitethernet 1/1 - 23
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Example (peGigE-Single Range)

This example shows single range configuration for PE Gigabit Ethernet ports.

```
Dell(conf)#interface range pegigE 1/0/3-14
Dell(conf-if-range-pegi-1/0/3-14)#
```

Example (Multiple Range)

This example shows how to use commas to add different interface types to the range enabling all 10-Gigabit Ethernet interfaces in the range 2/1 to 2/23 and both 10-Gigabit Ethernet interfaces 1/1 and 1/2.

```
Dell(config-if)# interface range tengigabitethernet 2/1-23, tengigabitethernet
1/1-2
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Example (Multiple Range)

This example shows how to use commas to add VLAN and port-channel interfaces to the range.

```
Dell(config-if)# interface range tengigabitethernet 2/1-23, tengigabitethernet
1/1-2,
Vlan 2-100, Port 1-25
Dell(config-if-range)# no shutdown
Dell(config-if-range)#
```

Related Commands

- interface port-channel — configures a port channel group.
- interface vlan — configures a VLAN interface.
- show config (from INTERFACE RANGE mode) — shows the bulk configuration interfaces.
- show range — shows the bulk configuration ranges.
- interface range macro (define) — defines a macro for an interface-range.

interface range macro (define)

Defines a macro for an interface range and then saves the macro in the running configuration.

C9000 Series

Syntax

```
define interface range macro name interface , interface , ...
```

Parameters

name	Enter up to 16 characters for the macro name.
interface, interface,...	Enter the keywords `interface range` and one of the interfaces — slot/port, pe-id/stack-unit/port-id, port-channel, or VLAN number. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. Comma-separated ranges can include VLANs, port-channels, and physical interfaces. Slot/Port information must contain a space before and after the dash. For example, `interface range tengigabitethernet 0/1 - 5` is valid; `interface range tengigabitethernet 0/1-5` is NOT valid. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094. • For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Added support for 4093 VLANs on E-Series ExaScale. Prior releases supported 2094.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Single Range)

This example shows how to define an interface range macro named test. Execute the `show running-config` command to display the macro definition.

```
Dell(config)# define interface-range test tengigabitethernet 0/0-3,
tengigabitethernet 1/0-47, tengigabitethernet 2/0-89

Dell# show running-config | grep define
define interface-range test tengigabitethernet 0/0-3, tengigabitethernet
1/0-47,
tengigabitethernet 2/0-89

Dell(config)#interface range macro test
Dell(config-if-range-te-0/0-3,te-1/0-47,te-2/0-89)#
```

Related Commands

- interface range – configures a range of command (bulk configuration)
- interface range macro name – runs an interface range macro.

interface range macro name

Run the interface-range macro to automatically configure the pre-defined range of interfaces.

C9000 Series

Syntax `interface range macro name`

Parameters

name	Enter the name of an existing macro.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced

Example (Single Range)

This example displays the macro named *test*.

```
Dell(config)# interface range macro test
Dell(config-if-range-te-0/0-3,te-1/0-47,te-2/0-89)#
Dell
```

Related Commands

- interface range — configures a range of command (bulk configuration).
- interface range macro (define) — defines a macro for an interface range (bulk configuration).

interface vlan

Configure a VLAN. You can configure up to 4094 VLANs.

C9000 Series

Syntax

```
interface vlan vlan-id
```

Parameters

vlan-id	Enter a number as the VLAN Identifier. The range is 1 to 4094.

Defaults

Not configured, except for the Default VLAN, which is configured as VLAN 1.

Command Modes

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0(1.3)	Introduced on the S5000.

Usage Information

For more information about VLANs and the commands to configure them, refer to the Virtual LAN (VLAN) Commands section of the Layer 2 chapter.

FTP, TFTP, and SNMP operations are not supported on a VLAN. MAC ACLs are not supported in VLANs. IP ACLs are supported. For more information, refer to the Access Control Lists (ACL) chapter.

Example (Single Range)

```
Dell(conf)# int vlan 3
Dell(conf-if-vl-3)#
```

Related Commands

- interface – configures a physical interface.
- interface loopback – configures a loopback interface.
- interface null – configures a null interface.
- interface port-channel – configures a port channel group.
- show vlan – displays the current VLAN configuration on the switch.
- shutdown – disables/enables the VLAN.
- tagged – adds a Layer 2 interface to a VLAN as a tagged interface.
- untagged – adds a Layer 2 interface to a VLAN as an untagged interface.

keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

C9000 Series

Syntax

`keepalive [seconds]`

To stop sending keepalive packets, use the `no keepalive` command.

Parameters

seconds	(OPTIONAL) For interfaces with PPP encapsulation enabled, enter the number of seconds between keepalive packets. The range is from 0 to 23767. The default is **10 seconds**.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.2	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.0	Introduced on the E-Series.

Usage Information When you configure `keepalive`, the system sends a self-addressed packet out of the configured interface to verify that the far end of a WAN link is up. When you configure `no keepalive`, the system does not send keepalive packets and so the local end of a WAN link remains up even if the remote end is down.

linecard portmode

Split a single 40G port into four 10G ports on the switch.

C9000 Series

Syntax `linecard slot-id port number portmode quad`

Parameters

linecard *slot-id*	Enter the slot ID of a line card to reset. The range of slot IDs is from 0 to 11.
number	Enter the port number of the 40G port to be split. The port range is from 0 to 20. A 40G port number is a multiple of 4; for example, 0, 4, 8, 12, ... 120, 124, 128).

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Usage Information Enabling quad mode on a port removes the interface configurations (if any) on the port after a save and reload. Be sure that the port is removed from other L2 and L3 feature configurations.

You must save and reload the system for the 40G to 4x10G port change to take effect.

This command cannot be used if LR4 optics are inserted in the 40G port.

monitor interface

Monitor counters on a single interface or all interfaces on a line card. The screen is refreshed every five seconds and the CLI prompt disappears.

C9000 Series

Syntax

`monitor interface [interface] [linecard slot-id]`

To disable monitoring and return to the CLI prompt, press the `q` key.

Parameters

interface (OPTIONAL) Enter the following keywords and slot/port or number information:

- For the management port, enter the keyword `managementethernet` then the slot (0 or 1) and the port (0).
- For a Tunnel interface, enter the keyword `tunnel` then the slot/port. The range is from 1 to 16383.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then the slot/port. The range is from 1 to 4094.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

linecard *slot-id* Enter the `linecard slot-id` parameters to specify the switch ports on a line card. The linecard slot ID range is from 0 to 11.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

In the Examples, the delta column displays changes since the last screen refresh.

The following are the `monitor` command menu options.

Key	Description
systest-3	Displays the host name assigned to the system.
monitor time	Displays the amount of time since the `monitor interface` command was entered.
time	Displays the amount of time the chassis is up (since last reboot).
m	Change the view from a single interface to all interfaces on the line card or visa-versa.
c	Refresh the view.
b	Change the counters displayed from Packets on the interface to Bytes.
r	Change the [delta] column from change in the number of packets/bytes in the last interval to rate per second.
l	Change the view to the next interface on the line card, or if in line card mode, the next line card in the chassis.
a	Change the view to the previous interface on the line card, or if in line card mode, the previous line card in the chassis.
T	Increase the screen refresh rate.
t	Decrease the screen refresh rate.
q	Return to the CLI prompt.

Example

```
Dell# monitor interface fortyGigE 2

  Dell Networking operating system uptime is 3 minute(s)
  Monitor time: 00:00:00   Refresh Intvl.: 2s

Interface   Link           In Packets         [delta]          Out
Packets         [delta]
   Fo 2/4     Up                    2               0
2               0
   Fo 2/8   Down                    0               0
0               0
  Fo 2/12   Down                    0               0
0               0
  Fo 2/16     Up                    1               0
1               0
  Fo 2/20     Up                    1               0
1               0
  Fo 2/24   Down                    0               0
0               0
```

```
  Fo 2/28     Up                    2               0
1               0
  Fo 2/32     Up                    1               0
2               0
  Fo 2/36   Down                    0               0
0               0
  Fo 2/40     Up                    0               0
2               0
  Fo 2/44     Up                    0               0
2               0
  Fo 2/48   Down                    0               0
0               0
  Fo 2/52   Down                    0               0
0               0
  Fo 2/56   Down                    0               0
0               0
  Fo 2/60   Down                    0               0
0               0
  Fo 2/64   Down                    0               0
0               0
  Fo 2/68   Down                    0               0
0               0
  Fo 2/72   Down                    0               0
0               0
  Fo 2/76   Down                    0               0
0               0
  Fo 2/80   Down                    0               0
0               0
  Fo 2/84   Down                    0               0
0               0
  Fo 2/88   Down                    0               0
0               0
  Fo 2/92   Down                    0               0
0               0
  Fo 2/96   Down                    0               0
0               0

       m - Change mode                          c - Clear screen
       b - Display bytes                        r - Display pkts/bytes per
sec
       l - Page up                              a - Page down
       T - Increase refresh interval            t - Decrease refresh interval
       q - Quit
```

```
Dell# monitor interface

  Dell Networking operating system uptime is 9 minute(s)
  Monitor time: 00:00:00   Refresh Intvl.: 2s

Interface   Link           In Packets         [delta]          Out
Packets         [delta]
   Te 1/0   Down                    0               0
0               0
   Te 1/1   Down                    0               0
0               0
   Te 2/2   Down                    0               0
0               0
   Te 2/3   Down                    0               0
0               0
   Fo 2/4     Up                   12               0
12              0
   Fo 2/8   Down                    0               0
0               0
  Fo 1/12   Down                    0               0
0               0
  Fo 1/16     Up                   11               0
11              0
  Fo 1/20     Up                   11               0
11              0
```

```
  Fo 2/24   Down                    0               0
0               0
  Fo 2/28     Up                   12               0
11              0
  Fo 2/32     Up                   11               0
12              0
  Fo 2/36   Down                    0               0
0               0
  Fo 2/40     Up                    0               0
13              0
  Fo 2/44     Up                    0               0
12              0
   Ma 0/0   Down                   17               0
1               0

       m - Change mode                           c - Clear screen
       b - Display bytes                         r - Display pkts/bytes per
sec
       l - Page up                               a - Page down
       T - Increase refresh interval             t - Decrease refresh interval
       q - Quit
```

```
Dell# monitor interface managementethernet 0/0

  Dell Networking operating system uptime is 4 minute(s)
  Monitor time: 00:00:00   Refresh Intvl.: 2s

 Interface: Ma 0/0, Enabled, Link is Down, Linespeed is auto

  Traffic statistics:              Current           Rate                 Delta
         Input bytes:                    0          0 Bps                    0
        Output bytes:                   42          0 Bps                    0
       Input packets:                    6          0 pps                    0
      Output packets:                    1          0 pps                    0
         64B packets:                    0          0 pps                    0
    Over 64B packets:                    0          0 pps                    0
   Over 127B packets:                    0          0 pps                    0
   Over 255B packets:                    0          0 pps                    0
   Over 511B packets:                    0          0 pps                    0
  Over 1023B packets:                    0          0 pps                    0
 Error statistics:
00:04:36: %RPM0-P:CP %CHMGR-5-PEM_INSERTED: Power entry module 3 of unit 0 is
inserted
     Input underruns:                    0          0 pps                    0
        Input giants:                    0          0 pps                    0
00:04:36: %RPM0-P:CP %CHMGR-0-PS_UP: Power supply 3 in unit 0 is up
     Input throttles:                    0          0 pps                    0
           Input CRC:                    0          0 pps                    0
   Input IP checksum:                    0          0 pps                    0
       Input overrun:                    0          0 pps                    0
    Output underruns:                    0          0 pps                    0
    Output throttles:                    0          0 pps                    0

       m - Change mode                           c - Clear screen
       l - Page up                               a - Page down
       T - Increase refresh interval             t - Decrease refresh interval
       q - Quit
```

mtu

Set the link maximum transmission unit (MTU) (frame size) for an Ethernet interface.

C9000 Series

Syntax

`mtu value`

To return to the default MTU value, use the `no mtu` command.

Parameters

value	Enter a maximum frame size in bytes. The range is from 594 to 9216. The default is **1554**.

Defaults

1554

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Reduced the maximum size of the maximum transmission unit (MTU) to 9216 bytes.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

If the packet includes a Layer 2 header, the difference between the link MTU and IP MTU (`ip mtu` command) must be enough bytes to include the Layer 2 header.

When you enter the `no mtu` command, the system reduces the IP MTU value to 1536 bytes.

Link MTU and IP MTU considerations for port channels and VLANs are as follows.

port channels:

- All members must have the same link MTU value and the same IP MTU value.
- The port channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the port channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

VLANs:

- All members of a VLAN must have same IP MTU value.
- Members can have different Link MTU values. Tagged members must have a link MTU 4 bytes higher than untagged members to account for the packet tag.
- The VLAN link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the VLAN members. For example, the VLAN contains tagged members with Link MTU of 1522 and IP MTU of 1500 and untagged members with Link MTU of 1518 and IP MTU of 1500. The VLAN's Link MTU cannot be higher than 1518 bytes and its IP MTU cannot be higher than 1500 bytes.

The following shows the difference between Link MTU and IP MTU.

Layer 2 Overhead	Link MTU and IP MTU Delta
Ethernet (untagged)	18 bytes
VLAN Tag	22 bytes
Untagged Packet with VLAN-Stack Header	22 bytes
Tagged Packet with VLAN-Stack Header	26 bytes

portmode hybrid

To accept both tagged and untagged frames, set a physical port or port-channel. A port configured this way is identified as a hybrid port in report displays.

C9000 Series

Syntax

```
portmode hybrid
```

To return a port to accept either tagged or untagged frames (non-hybrid), use the `no portmode hybrid` command.

Defaults

non-hybrid

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

The following describes the `interface` command shown in the following example. This example sets a port as hybrid, makes the port a tagged member of VLAN 20, and an untagged member of VLAN 10, which becomes the native VLAN of the port. The port now accepts:

- untagged frames and classify them as VLAN 10 frames
- VLAN 20 tagged frames

The following describes the `do show interfaces` command shown in the following example. This example shows output with "Hybrid" as the newly added value for 802.1QTagged. The options for this field are:

- True — port is tagged
- False — port is untagged
- Hybrid — port accepts both tagged and untagged frames

The following describes the `interface vlan` command shown in the following example. This example shows unconfiguration of the hybrid port using the `no portmode hybrid` command.

NOTE: Remove all other configurations on the port before you can remove the hybrid configuration from the port.

Example

```
Dell(conf)# interface te 2/0
Dell(conf-if-te-2/0)# portmode hybrid
Dell(conf-if-te-2/0)# interface vlan 10
Dell(conf-if-vl-10)# untagged te 2/0
Dell(conf-if-vl-10)# interface vlan 20
Dell(conf-if-vl-20)# tagged te 2/0
Dell(conf-if-vl-20)#
```

Example

```
Dell(conf-if-vl-20)# do show interfaces switchport
Name: TenGigabitEthernet 2/0
802.1QTagged: Hybrid
Vlan membership:
Vlan  10,   Vlan 20
Native   VlanId: 10
Dell(conf-if-vl-20)#
```

Example (Vlan)

```
Dell(conf-if-vl-20)# interface vlan 10
Dell(conf-if-vl-10)# no untagged te 2/0
Dell(conf-if-vl-10)# interface vlan 20
Dell(conf-if-vl-20)# no tagged te 2/0
Dell(conf-if-vl-20)# interface te 2/0
Dell(conf-if-te-2/0)# no portmode hybrid
Dell(conf-if-vl-20)#
```

Related Commands

- show interfaces switchport — displays the configuration of switchport (Layer 2) interfaces on the switch.
- switchport — places the interface in a Layer 2 mode.
- vlan-stack trunk — specifies an interface as a trunk port to the Stackable VLAN network.

rate-interval

Configure the traffic sampling interval on the selected interface.

C9000 Series

Syntax `rate-interval seconds`

Parameters

seconds — Enter the number of seconds for which to collect traffic data. The range is from 5 to 299 seconds.

NOTE: Because polling occurs every 15 seconds, the number of seconds designated here rounds to the multiple of 15 seconds lower than the entered value. For example, if 44 seconds is designated, it rounds to 30; 45 to 59 seconds rounds to 45.

Defaults **299 seconds**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced

Usage Information The output of the `show interfaces` command displays the configured rate interval, along with the collected traffic data.

Related Commands show interfaces — displays information on physical and virtual interfaces.

rate-interval (Configuration Mode)

Configure the traffic sampling interval for all physical and logical port-channel interfaces globally. The support to configure rate-interval globally enables you to modify the default interval rate for all physical and logical interfaces at one time.

Syntax

`rate-interval seconds`

Use the `no rate-interval` command to remove the sampling interval configuration.

Parameters

seconds — Enter the number of seconds for which to collect traffic data. The range is from 5 to 299 seconds.

NOTE: Because polling occurs every 15 seconds, the number of seconds designated here round to the multiple of 15 seconds lower than the entered value. For example, if 44 seconds is designated, it rounds to 30; 45 to 59 seconds rounds to 45. If you configure this value to be less than 5, then the entire buffer is cleared; the `show int stats` command shows the rate information to be 0 as the polling interval is less than 5.

Defaults

299 seconds

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11.0.0	Introduced on all Dell Networking OS platforms.

Usage Information

The output of the `show interfaces` command displays the configured rate interval, along with the collected traffic data.

When rate-interval is not configured in the global configuration mode or interface mode, the default value of 299 seconds is applied.

When rate-interval is configured only in the global configuration mode and not in the interface mode, the global rate-interval value is applied at the interface level also.

When rate-interval is configured at the interface level and not in the global configuration mode, the interface level rate-interval value is applied for an interface.

When rate interval is configured in both global configuration mode as well as interface mode, then the rate-interval value configured at interface level is applied as it takes precedence over the global value.

show config

Display the interface configuration.

C9000 Series

Syntax `show config`

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Example

```
Dell(conf)#int peg 255/1/0
Dell(conf-if-pegi-255/1/0)#sho con
!
interface peGigE 255/1/0
 dampening 20 200 800 80
 no shutdown
```

```
Dell(conf-if)# show conf
!
interface TenGigabitEthernet 1/7
  no ip address
  switchport
  no shutdown
Dell(conf-if)#
```

show config (from INTERFACE RANGE mode)

Display the bulk configured interfaces (`interface range`).

C9000 Series

Syntax `show config`

Command Modes INTERFACE RANGE (conf-if-range)

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell(conf)# interface range tengigabitethernet 1/1 - 2
Dell(conf-if-range-te-1/1-2)# show config
!
interface TenGigabitEthernet 1/1
  no ip address
  switchport
  no shutdown
!
interface TenGigabitEthernet 1/2
  no ip address
  switchport
  no shutdown
Dell(conf-if-range-te-1/1-2)#
```

show interfaces

Display information on a specific physical or virtual interface, or the interfaces of the same type on a line card.

C9000 Series

Syntax

`show interfaces [interface] [linecard slot-id]`

From a **PE console**, use `show interfaces` to view the information on a specific physical or virtual interface.

Parameters

interface

Enter one of the following keywords and slot/port or number information:

- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is 1 to 4096.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

NOTE: The peGigE or peTenGigE option is only visible when the feature extended bridge feature is enabled.

linecard *slot-id*

Enter the `linecard slot-id` parameters to specify the switch ports on a line card. The range of slot IDs is from 0 to 11.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Added support for the tunnel interface type.
9.1(0.0)	Updated ManagementEthernet output to include two global IPv6 addresses on S4810 and Z9000 and added output example showing OpenFlow instance ID.
8.3.12.1	Updated command output to support multiple IPv6 addresses on S4810.
8.3.11.4	Output expanded to support eSR4 optics in Z9000.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.2	Included SFP and SFP+ optics power detail in the E-Series and C-Series output.
8.2.1.0	Added support for 4093 VLANs on the E-Series ExaScale. Prior releases supported 2094.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Output expanded to include SFP+ media on the C-Series.
7.6.1.0	Introduced on the S Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Changed the organization of the display output.
6.3.1.0	Added the Pluggable Media Type field in the E-Series TeraScale output.

Usage Information

Use the `show interfaces` command for details on a specific interface. Use the `show interfaces linecard` command for details on all interfaces on the designated line card.

NOTE: In the CLI output, the power value is rounded to a 3-digit value. For receive/transmit power that is less than 0.000, an `snmp query` returns the corresponding dbm value even though the CLI displays as 0.000.

NOTE: After the counters are cleared, the line-rate continues to increase until it reaches the maximum line rate. When the maximum line rate is reached, there is no change in the line-rate.

The following table describes the `show interfaces` command shown in the 10G example.

Line	Description
TenGigabitEthernet 0/0...	Interface type, slot/port, and administrative and line protocol status.
Hardware is...	Interface hardware information, assigned MAC address, and current address.
Pluggable media present...	Present pluggable media wavelength, type, and rate. The error scenarios are: • Wavelength, Non-qualified — Dell Force10 ID is not present, but wavelength information is available from XFP or SFP serial data • Wavelength, F10 unknown—Dell Force10 ID is present, but not able to determine the optics type • Unknown, Non-qualified— if wavelength is reading error, and F10 ID is not present

Line	Description
	Dell Networking allows unsupported SFP and XFP transceivers to be used, but the system might not be able to retrieve some data about them. In that case, typically when the output of this field is "Pluggable media present, Media type is unknown", the Medium and the XFP/SFP receive power reading data might not be present in the output.
Interface index...	Displays the interface index number used by SNMP to identify the interface.
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
MTU 1554...	Displays link and IP MTU information.
LineSpeed	Displays the interface's line speed, duplex mode, and Slave.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the `show interfaces` counters where cleared.
Queuing strategy...	States the packet queuing strategy. FIFO means first in first out.
Input Statistics:	Displays all the input statistics including: • Number of packets and bytes into the interface • Number of packets with VLAN tagged headers • Packet size and the number of those packets inbound to the interface • Number of Multicast and Broadcast packets: – Multicasts = number of MAC multicast packets – Broadcasts = number of MAC broadcast packets • Number of runts, giants, and throttles packets: – runts = number of packets that are less than 64B – giants = packets that are greater than the MTU size – throttles = packets containing PAUSE frames • Number of CRC, overrun, and discarded packets: – CRC = packets with CRC/FCS errors – overrun = number of packets discarded due to FIFO overrun conditions – discarded = the sum of runts, giants, CRC, and overrun packets discarded without any processing
Output Statistics:	Displays output statistics sent out of the interface including: • Number of packets, bytes, and underruns out of the interface • Packet size and the number of those packets outbound to the interface • Number of Multicast, Broadcast, and Unicast packets: – Multicasts = number of MAC multicast packets – Broadcasts = number of MAC broadcast packets – Unicasts = number of MAC unicast packets • Number of VLANs, throttles, discards, and collisions:: – Vlans = number of VLAN tagged packets – throttles = packets containing PAUSE frames – discarded = number of packets discarded without any processing – collisions = number of packet collisions

Line	Description
	– wred=count both packets discarded in the MAC and in the hardware-based queues
Rate information...	Estimate of the input and output traffic rate over a designated interval (30 to 299 seconds). Traffic rate is displayed in bits, packets per second, and percent of line rate.
Time since...	Elapsed time since the last interface status change (hh:mm:ss format).

Example

```
Dell# show interfaces
TenGigabitEthernet 2/0 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
    Current address is 74:86:7a:ff:6f:18
Pluggable media present, Media type is unknown
    Wavelength is 0.00nm
Interface index is 151060994
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:08:58
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:07:34
```

Usage Information

The Management port is enabled by default (`no shutdown`). If necessary, use the `ip address` command to assign an IP address to the Management port. If two RPMs are installed in your system, use the `show redundancy` command to display which RPM is the Primary RPM.

You can configure two global IPv6 addresses. To view the addresses, use the `show interface managementethernet` command. If you try to configure a third IPv6 address, a message displays. If auto-configuration is enabled, all IPv6 addresses on that management interface are auto-configured. The first IPv6 address that is configured on the management interface is the primary address. If deleted, it must be re-added; the secondary address is not promoted.

To view information on a specific PE stack-unit, use the `show interface pe` *`pe-id`* `stack unit` *unit-number* command. You can use the `show interfaces peGigE` command to view the information on all the components of the PE Gigabit Ethernet interface. You can use the `show interfaces peTenGigE` command to view the information on all the components of the PE 10–Gigabit Ethernet interface.

To view the show output for multiple ports of a specified slot at a time, you can specify any random port number or a range of ports, or a combination of both.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces FortyGigE 1/0-4,7,9-11`. To enter any random number of ports, you can enter a comma-separated string of port numbers, for example `show interfaces FortyGigE 1/0/1,9,11`

NOTE: The port-range option is only available for 1 Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, Fast Ethernet, FC, Port Channel, and VLAN interfaces.

Example (TenGigabit Interface)

```
Dell# show interfaces tengigabitethernet 2
TenGigabitEthernet 2/0 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
    Current address is 74:86:7a:ff:6f:18
Pluggable media present, Media type is unknown
    Wavelength is 0.00nm
Interface index is 151060994
Backup Interface of this port is Te 2/1
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:22:49
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 01:21:35


TenGigabitEthernet 2/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
    Current address is 74:86:7a:ff:6f:18
Pluggable media present, Media type is unknown
    Wavelength is 0.00nm
Interface index is 151323138
Backup Interface of this port is Te 2/0
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10000 Mbit
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:22:49
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,         0 packets/sec, 0.00% of line-rate
Time since last interface status change: 01:21:35


TenGigabitEthernet 2/2 is down, line protocol is down
Hardware is DellForce10Eth, address is 74:86:7a:ff:6f:18
    Current address is 74:86:7a:ff:6f:18
```

Example (TenGigabit Interface— range of ports)

```
Dell#show interface tengigabitethernet 6/1-4
TenGigabitEthernet 6/1 is up, line protocol is up
Port is part of Port-channel 513
Hardware is DellEth, address is 34:17:eb:00:20:94
    Current address is 34:17:eb:00:20:94
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    SFP+ receive power reading is -1.7354dBm
Interface index is 7340164
Interface mode is Cascade
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002094
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 10000 Mbit
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 02:26:09
Queueing strategy: fifo
Input Statistics:
     1706746618 packets, 1364807638007 bytes
     0 64-byte pkts, 63573150 over 64-byte pkts, 150696430 over 127-byte pkts
     301583958 over 255-byte pkts, 600606507 over 511-byte pkts, 590286573
over 1023-byte pkts
     20633 Multicasts, 0 Broadcasts, 1706725970 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     1597676771 packets, 1279964238742 bytes, 0 underruns
     0 64-byte pkts, 58135245 over 64-byte pkts, 140947056 over 127-byte pkts
     282053890 over 255-byte pkts, 562259268 over 511-byte pkts, 554281312
over 1023-byte pkts
     2807 Multicasts, 0 Broadcasts, 1597673964 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 1320.00 Mbits/sec,     206410 packets/sec, 13.53% of line-rate
     Output 1237.00 Mbits/sec,     193181 packets/sec, 12.68% of line-rate
Time since last interface status change: 02:19:12


TenGigabitEthernet 6/2 is down, line protocol is down
Hardware is DellEth, address is 34:17:eb:00:20:95
    Current address is 34:17:eb:00:20:95
Pluggable media present, Media type is unknown
    Wavelength unknown
Interface index is 7340292
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002095
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 02:27:00
Queueing strategy: fifo
```

```
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 02:26:59


TenGigabitEthernet 6/3 is down, line protocol is down
Hardware is DellEth, address is 34:17:eb:00:20:96
    Current address is 34:17:eb:00:20:96
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    No power
Interface index is 7340420
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002096
Dell#show interface tengigabitethernet 6/1-11
TenGigabitEthernet 6/1 is up, line protocol is up
Port is part of Port-channel 513
Hardware is DellEth, address is 34:17:eb:00:20:94
    Current address is 34:17:eb:00:20:94
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    SFP+ receive power reading is -1.7347dBm
Interface index is 7340164
Interface mode is Cascade
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002094
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 10000 Mbit
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 02:26:52
Queueing strategy: fifo
Input Statistics:
     1715563966 packets, 1371858136501 bytes
     0 64-byte pkts, 63901828 over 64-byte pkts, 151474752 over 127-byte pkts
     303141318 over 255-byte pkts, 603711156 over 511-byte pkts, 593334912
over 1023-byte pkts
     20742 Multicasts, 0 Broadcasts, 1715543204 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     1605928396 packets, 1286578165117 bytes, 0 underruns
     0 64-byte pkts, 58435170 over 64-byte pkts, 141674160 over 127-byte pkts
     283509010 over 255-byte pkts, 565163364 over 511-byte pkts, 557146692
over 1023-byte pkts
     2821 Multicasts, 0 Broadcasts, 1605925575 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 1320.00 Mbits/sec,     206386 packets/sec, 13.53% of line-rate
     Output 1237.00 Mbits/sec,     193157 packets/sec, 12.68% of line-rate
Time since last interface status change: 02:19:55
```

```
TenGigabitEthernet 6/4 is down, line protocol is down
Hardware is DellEth, address is 34:17:eb:00:20:97
    Current address is 34:17:eb:00:20:97
Pluggable media present, Media type is unknown
    Wavelength unknown
Interface index is 7340548
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002097
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 02:27:42
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 02:27:41
```

Example (TenGigabit Interface— random ports)

```
Dell#show interfaces tengigabitethernet 6/1,3
TenGigabitEthernet 6/1 is up, line protocol is up
Port is part of Port-channel 513
Hardware is DellEth, address is 34:17:eb:00:20:94
    Current address is 34:17:eb:00:20:94
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    SFP+ receive power reading is -1.7685dBm
Interface index is 7340164
Interface mode is Cascade
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002094
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 10000 Mbit
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 02:33:46
Queueing strategy: fifo
Input Statistics:
     1800663963 packets, 1439907147651 bytes
     0 64-byte pkts, 67073349 over 64-byte pkts, 158991672 over 127-byte pkts
     318176170 over 255-byte pkts, 633651831 over 511-byte pkts, 622770941 over
1023-byte pkts
     21764 Multicasts, 0 Broadcasts, 1800642183 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     1685574635 packets, 1350380268687 bytes, 0 underruns
     0 64-byte pkts, 61338933 over 64-byte pkts, 148705670 over 127-byte pkts
     297567447 over 255-byte pkts, 593182373 over 511-byte pkts, 584780212 over
1023-byte pkts
     2956 Multicasts, 0 Broadcasts, 1685571679 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
```

```
Rate info (interval 299 seconds):
     Input 1320.00 Mbits/sec,     206454 packets/sec, 13.53% of line-rate
     Output 1238.00 Mbits/sec,     193222 packets/sec, 12.69% of line-rate
Time since last interface status change: 02:26:50


TenGigabitEthernet 6/3 is down, line protocol is down
Hardware is DellEth, address is 34:17:eb:00:20:96
    Current address is 34:17:eb:00:20:96
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    No power
Interface index is 7340420
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002096
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 02:34:38
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 02:34:37
```

Example (VLAN Interface)

```
Dell# show interfaces vlan 1
Vlan 1 is down, line protocol is down
Address is 74:86:7a:ff:6f:18, Current address is 74:86:7a:ff:6f:18
Interface index is 1124302849
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 01:22:55
Queueing strategy: fifo
Time since last interface status change: 01:22:55
```

Example (ManagementEthernet Interface with two IPv6 addresses)

```
Dell# show interfaces managementethernet 0/0

ManagementEthernet 0/0 is up, line protocol is up

Hardware is DellForce10Eth, address is 00:01:e8:a0:bf:f3

Current address is 00:01:e8:a0:bf:f3

Pluggable media not present

Interface index is 302006472

Internet address is 10.16.130.5/16
```

```
Link local IPv6 address: fe80::201:e8ff:fea0:bff3/64

Global IPv6 address: 1::1/

Global IPv6 address: 2::1/64

Virtual-IP is not set

Virtual-IP IPv6 address is not set

MTU 1554 bytes, IP MTU 1500 bytes

LineSpeed 1000 Mbit, Mode full duplex

ARP type: ARPA, ARP Timeout 04:00:00

Last clearing of "show interface" counters 00:06:14

Queueing strategy: fifo

Input 791 packets, 62913 bytes, 775 multicast

Received 0 errors, 0 discarded

Output 21 packets, 3300 bytes, 20 multicast

Output 0 errors, 0 invalid protocol

Time since last interface status change: 00:06:03
```

Example (PE Gigabit Ethernet Interface)

```
Dell#show interfaces peGigE 0/0/1
peGigE 0/0/1 is up, line protocol is up
Hardware is DellEth, address is a0:68:00:3f:92:bd
    Current address is a0:68:00:3f:92:bd
Pluggable media not present
Interface index is 536870919
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :a068003f92bd
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex
Auto-mdix enabled, ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 02:44:11
Queueing strategy: fifo
Input Statistics:
     5150004 packets, 4996095648 bytes
     164432 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
     0 over 255-byte pkts, 4985572 over 511-byte pkts, 0 over 1023-byte pkts
     0 Multicasts, 0 Broadcasts, 5150004 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     11165065 packets, 714564160 bytes, 0 underruns
     11165065 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
     309 Multicasts, 0 Broadcasts, 11164756 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 140.00 Mbits/sec,      18070 packets/sec, 14.30% of line-rate
     Output 20.00 Mbits/sec,      39175 packets/sec, 2.60% of line-rate
Time since last interface status change: 02:37:06
```

Example (PE TenGigabit Ethernet Interface)

```
Dell#show interfaces petenGigE 21/0/49
peTenGigE 21/0/49 is down, line protocol is down
Hardware is DellEMCEth, address is 00:00:00:00:00:00
    Current address is 00:00:00:00:00:00
Pluggable media not present
    No transmit power
Interface index is 558915592
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :000000000000
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:00:00
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:14:41
```

Example (PE Console)

```
Dell#show interfaces
TenGigabitEthernet 0/1 is up, line protocol is not present
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
Interface index is 1054730
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 1000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:00:00
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d20h19m


TenGigabitEthernet 0/2 is up, line protocol is not present
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
```

```
Interface index is 1054858
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 1000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:00:00
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d20h19m


TenGigabitEthernet 1/1 is up, line protocol is up
Port is part of Port-channel 257
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    No power
Interface index is 2103306
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 10000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 6d20h19m
Queueing strategy: fifo
Input Statistics:
     4062996 packets, 799504603 bytes
     0 64-byte pkts, 193370 over 64-byte pkts, 3869429 over 127-byte pkts
     2 over 255-byte pkts, 20 over 511-byte pkts, 175 over 1023-byte pkts
     193229 Multicasts, 0 Broadcasts, 3869767 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     3978357 packets, 4298183062 bytes, 0 underruns
     0 64-byte pkts, 110 over 64-byte pkts, 187904 over 127-byte pkts
     94 over 255-byte pkts, 17498 over 511-byte pkts, 3772751 over 1023-byte
pkts
     187593 Multicasts, 0 Broadcasts, 3790764 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d20h19m


TenGigabitEthernet 1/2 is up, line protocol is down
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
Pluggable media not present
Interface index is 2103434
```

```
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 6d21h14m
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d21h13m


TenGigabitEthernet 2/1 is up, line protocol is not present
Hardware is DellEth, address is f8:b1:56:62:61:0a
    Current address is f8:b1:56:62:61:0a
Interface index is 3151882
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 1000 Mbit
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:00:00
Queueing strategy: fifo
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes, 0 underruns
     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 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d21h12m

Port-channel 257 is up, line protocol is up
Created by Auto LAG
Hardware address is f8:b1:56:62:61:0a, Current address is f8:b1:56:62:61:0a
Interface index is 1258422784
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed 10000 Mbit
Members in this channel:  Te 1/1(U)
ARP type: ARPA, ARP Timeout 04:00:00
```

```
Queueing strategy: fifo
Input Statistics:
     4062996 packets, 799504603 bytes
     0 64-byte pkts, 193370 over 64-byte pkts, 3869429 over 127-byte pkts
     2 over 255-byte pkts, 20 over 511-byte pkts, 175 over 1023-byte pkts
     193229 Multicasts, 0 Broadcasts, 3869767 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     3978357 packets, 4298183062 bytes, 0 underruns
     0 64-byte pkts, 110 over 64-byte pkts, 187904 over 127-byte pkts
     94 over 255-byte pkts, 17498 over 511-byte pkts, 3772751 over 1023-byte
pkts
     187593 Multicasts, 0 Broadcasts, 3790764 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 6d21h13m


Vlan 1 is down, line protocol is down
Address is f8:b1:56:62:61:0a, Current address is f8:b1:56:62:61:0a
Interface index is 1275068928
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :f8b15662610a
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 6d21h13m
Queueing strategy: fifo
Time since last interface status change: 6d21h13m
```

Related Commands

- show interfaces configured – displays any interface with a non-default configuration.
- show interfaces switchport – displays Layer 2 information about the interfaces.
- show inventory (S-Series and Z-Series) – displays the S Series and Z-Series switch types, components (including media), Dell Networking OS version including hardware identification numbers, and configured protocols.
- show ip interface – displays Layer 3 information about the interfaces.
- show range – displays all interfaces configured using the interface range command.

show interfaces configured

Display any interface with a non-default configuration.

C9000 Series

Syntax `show interfaces configured`

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Changed the organization of the display output.

```
Dell#show interfaces configured | no-more
TenGigabitEthernet 6/0 is up, line protocol is down
Hardware is DellEth, address is 34:17:eb:00:20:93
    Current address is 34:17:eb:00:20:93
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    SFP+ receive power reading is -2.0350dBm
Interface index is 7340036
Interface mode is Cascade
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002093
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 04:24:38
Queueing strategy: fifo
Input Statistics:
     20998409 packets, 16779063804 bytes
     0 64-byte pkts, 806642 over 64-byte pkts, 1847316 over 127-byte pkts
     3696420 over 255-byte pkts, 7384764 over 511-byte pkts, 7263267 over 1023-
byte pkts
     177 Multicasts, 0 Broadcasts, 20998232 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     753 packets, 65838 bytes, 0 underruns
     0 64-byte pkts, 744 over 64-byte pkts, 1 over 127-byte pkts
     1 over 255-byte pkts, 6 over 511-byte pkts, 1 over 1023-byte pkts
     184 Multicasts, 0 Broadcasts, 569 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 04:15:18


TenGigabitEthernet 6/1 is up, line protocol is down
Hardware is DellEth, address is 34:17:eb:00:20:94
    Current address is 34:17:eb:00:20:94
Pluggable media present, SFP+ type is 10GBASE-SR
    Medium is MultiRate, Wavelength is 850nm
    SFP+ receive power reading is -1.8762dBm
Interface index is 7340164
Interface mode is Cascade
Internet address is not set
```

```
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002094
MTU 16364 bytes, IP MTU 16346 bytes
LineSpeed auto
Flowcontrol rx off tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 04:24:39
Queueing strategy: fifo
Input Statistics:
     20998413 packets, 16777169337 bytes
     0 64-byte pkts, 807800 over 64-byte pkts, 1848271 over 127-byte pkts
     3694162 over 255-byte pkts, 7388878 over 511-byte pkts, 7259302 over 1023-
byte pkts
     177 Multicasts, 0 Broadcasts, 20998236 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     21135427 packets, 16886701995 bytes, 0 underruns
     0 64-byte pkts, 813148 over 64-byte pkts, 1860008 over 127-byte pkts
     3718428 over 255-byte pkts, 7437164 over 511-byte pkts, 7306679 over 1023-
byte pkts
     184 Multicasts, 0 Broadcasts, 21135243 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 04:15:18

peGigE 255/1/1 is up, line protocol is up
Hardware is DellEth, address is 34:17:eb:00:bb:8a
    Current address is 34:17:eb:00:bb:8a
Pluggable media not present
Interface index is 804323847
Dampening suppression is ON for this interface
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb00bb8a
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex
Auto-mdix enabled, ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:57:53
Queueing strategy: fifo
Input Statistics:
     110 packets, 7040 bytes
     110 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
     110 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     110 packets, 7040 bytes, 0 underruns
     110 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
     110 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:55:34


peGigE 255/1/2 is up, line protocol is up
Hardware is DellEth, address is 34:17:eb:00:bb:8b
    Current address is 34:17:eb:00:bb:8b
Pluggable media not present
Interface index is 804324359
Dampening suppression is ON for this interface
Internet address is not set
Mode of IPv4 Address Assignment : NONE
```

```
DHCP Client-ID :3417eb00bb8b
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex
Auto-mdix enabled, ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 00:57:53
Queueing strategy: fifo
Input Statistics:
     111 packets, 7104 bytes
     111 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
     111 Multicasts, 0 Broadcasts, 0 Unicasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     111 packets, 7104 bytes, 0 underruns
     111 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
     111 Multicasts, 0 Broadcasts, 0 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
Time since last interface status change: 00:55:34
```

Related Commands show interfaces — displays information on a specific physical interface or virtual interface.

show interfaces dampening

Display interface dampening information.

C9000 Series

Syntax `show interfaces dampening [[interface] [summary] [detail]]`

Parameters

interface (Optional) Enter one of the following keywords and slot/port or number information:

- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

NOTE: The peGigE or peTenGigE output is only visible when the feature extended bridge feature is enabled.

summary	(OPTIONAL) Enter the keyword `summary` to display the current summary of dampening data, including the number of interfaces configured and the number of interfaces suppressed, if any.
detail	(OPTIONAL) Enter the keyword `detail` to display detailed interface dampening data.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced

Usage Information To view the show output for multiple ports of a specified slot at a time, you can specify any random port number or a range of ports, or a combination of both.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces dampening FortyGigE 1/0-4,7,9-11`. To enter any random number of ports, you can enter a comma-separated string of port numbers, for example `show interfaces dampening FortyGigE 1/0/1,9,11`

NOTE: The port-range option is only available for 1 Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, Fast Ethernet, FC, Port Channel, and VLAN interfaces.

Example show interfaces dampening (peGigE)

```
Dell#show interfaces dampening
Interface       Supp    Flaps   Penalty Half-Life   Reuse   Suppress    Max-Sup
                State
PeGi 255/1/1    Up      0       0       20          200     800         80
PeGi 255/1/2    Up      0       0       20          200     800         80
PeGi 255/1/3    Up      0       0       20          200     800         80
PeGi 255/1/4    Up      0       0       20          200     800         80
PeGi 255/1/5    Up      0       0       20          200     800         80
PeGi 255/1/6    Up      0       0       20          200     800         80
PeGi 255/1/7    Up      0       0       20          200     800         80
PeGi 255/1/8    Up      0       0       20          200     800         80
PeGi 255/1/9    Up      0       0       20          200     800         80
PeGi 255/1/10   Up      0       0       20          200     800         80
PeGi 255/1/11   Up      0       0       20          200     800         80
PeGi 255/1/12   Up      0       0       20          200     800         80
```

```
PeGi 255/1/13   Up      0       0       20          200     800         80
PeGi 255/1/14   Up      0       0       20          200     800         80
PeGi 255/1/15   Up      0       0       20          200     800         80
PeGi 255/1/16   Up      0       0       20          200     800         80
PeGi 255/1/17   Up      0       0       20          200     800         80
PeGi 255/1/18   Up      0       0       20          200     800         80
PeGi 255/1/19   Up      0       0       20          200     800         80
PeGi 255/1/20   Up      0       0       20          200     800         80
PeGi 255/1/21   Up      0       0       20          200     800         80
PeGi 255/1/22   Up      0       0       20          200     800         80
PeGi 255/1/23   Up      0       0       20          200     800         80
PeGi 255/1/24   Up      0       0       20          200     800         80
PeGi 255/1/25   Up      0       0       20          200     800         80
PeGi 255/1/26   Up      0       0       20          200     800         80
PeGi 255/1/27   Up      0       0       20          200     800         80
PeGi 255/1/28   Up      0       0       20          200     800         80
PeGi 255/1/29   Up      0       0       20          200     800         80
PeGi 255/1/30   Up      0       0       20          200     800         80
PeGi 255/1/31   Up      0       0       20          200     800         80
PeGi 255/1/32   Up      0       0       20          200     800         80
PeGi 255/1/33   Up      0       0       20          200     800         80
PeGi 255/1/34   Up      0       0       20          200     800         80
PeGi 255/1/35   Up      0       0       20          200     800         80
PeGi 255/1/36   Up      1       0       20          200     800         80
PeGi 255/1/37   Up      1       0       20          200     800         80
PeGi 255/1/38   Up      0       0       20          200     800         80
PeGi 255/1/39   Up      0       0       20          200     800         80
PeGi 255/1/40   Up      0       0       20          200     800         80
PeGi 255/1/41   Up      0       0       20          200     800         80
PeGi 255/1/42   Up      0       0       20          200     800         80
PeGi 255/1/43   Up      0       0       20          200     800         80
PeGi 255/1/44   Up      0       0       20          200     800         80
PeGi 255/1/45   Up      0       0       20          200     800         80
PeGi 255/1/46   Up      0       0       20          200     800         80
PeGi 255/1/47   Up      0       0       20          200     800         80
PeGi 255/1/48   Up      0       0       20          200     800         80
PeGi 255/2/1    Up      0       0       20          200     800         80
PeGi 255/2/2    Up      1       0       20          200     800         80
PeGi 255/2/3    Up      1       0       20          200     800         80
PeGi 255/2/4    Up      1       0       20          200     800         80
PeGi 255/2/5    Up      1       0       20          200     800         80
PeGi 255/2/6    Up      1       0       20          200     800         80
PeGi 255/2/7    Up      1       0       20          200     800         80
PeGi 255/2/8    Up      1       0       20          200     800         80
PeGi 255/2/9    Up      1       0       20          200     800         80
PeGi 255/2/10   Up      1       0       20          200     800         80
PeGi 255/2/11   Up      1       0       20          200     800         80
PeGi 255/2/12   Up      1       0       20          200     800         80
PeGi 255/2/13   Up      1       0       20          200     800         80
PeGi 255/2/14   Up      1       0       20          200     800         80
PeGi 255/2/15   Up      1       0       20          200     800         80
PeGi 255/2/16   Up      1       0       20          200     800         80
PeGi 255/2/17   Up      1       0       20          200     800         80
PeGi 255/2/18   Up      1       0       20          200     800         80
PeGi 255/2/19   Up      1       0       20          200     800         80
PeGi 255/2/20   Up      1       0       20          200     800         80
PeGi 255/2/21   Up      1       0       20          200     800         80
PeGi 255/2/22   Up      1       0       20          200     800         80
PeGi 255/2/23   Up      1       0       20          200     800         80
PeGi 255/2/24   Up      1       0       20          200     800         80
PeGi 255/2/25   Up      1       0       20          200     800         80
PeGi 255/2/26   Up      1       0       20          200     800         80
PeGi 255/2/27   Up      1       0       20          200     800         80
PeGi 255/2/28   Up      1       0       20          200     800         80
PeGi 255/2/29   Up      1       0       20          200     800         80
PeGi 255/2/30   Up      1       0       20          200     800         80
PeGi 255/2/31   Up      1       0       20          200     800         80
PeGi 255/2/32   Up      1       0       20          200     800         80
PeGi 255/2/33   Up      1       0       20          200     800         80
PeGi 255/2/34   Up      1       0       20          200     800         80
PeGi 255/2/35   Up      1       0       20          200     800         80
PeGi 255/2/36   Up      1       0       20          200     800         80
PeGi 255/2/37   Up      1       0       20          200     800         80
PeGi 255/2/38   Up      1       0       20          200     800         80
PeGi 255/2/39   Up      1       0       20          200     800         80
PeGi 255/2/40   Up      1       0       20          200     800         80
PeGi 255/2/41   Up      1       0       20          200     800         80
```

```
PeGi 255/2/42   Up      1       0       20          200     800         80
PeGi 255/2/43   Up      1       0       20          200     800         80
PeGi 255/2/44   Up      1       0       20          200     800         80
PeGi 255/2/45   Up      1       0       20          200     800         80
PeGi 255/2/46   Up      0       0       20          200     800         80
PeGi 255/2/47   Up      0       0       20          200     800         80
PeGi 255/2/48   Up      0       0       20          200     800         80
PeGi 255/3/1    Up      1       0       20          200     800         80
PeGi 255/3/2    Up      1       0       20          200     800         80
PeGi 255/3/3    Up      1       0       20          200     800         80
PeGi 255/3/4    Up      1       0       20          200     800         80
PeGi 255/3/5    Up      1       0       20          200     800         80
PeGi 255/3/6    Up      1       0       20          200     800         80
PeGi 255/3/7    Up      1       0       20          200     800         80
PeGi 255/3/8    Up      1       0       20          200     800         80
PeGi 255/3/9    Up      1       0       20          200     800         80
PeGi 255/3/10   Up      1       0       20          200     800         80
PeGi 255/3/11   Up      1       0       20          200     800         80
PeGi 255/3/12   Up      1       0       20          200     800         80
PeGi 255/3/13   Up      1       0       20          200     800         80
PeGi 255/3/14   Up      1       0       20          200     800         80
PeGi 255/3/15   Up      1       0       20          200     800         80
PeGi 255/3/16   Up      1       0       20          200     800         80
PeGi 255/3/17   Up      1       0       20          200     800         80
PeGi 255/3/18   Up      1       0       20          200     800         80
PeGi 255/3/19   Up      1       0       20          200     800         80
PeGi 255/3/20   Up      1       0       20          200     800         80
PeGi 255/3/21   Up      1       0       20          200     800         80
PeGi 255/3/22   Up      1       0       20          200     800         80
PeGi 255/3/23   Up      1       0       20          200     800         80
PeGi 255/3/24   Up      1       0       20          200     800         80
PeGi 255/3/25   Up      1       0       20          200     800         80
PeGi 255/3/26   Up      1       0       20          200     800         80
PeGi 255/3/27   Up      1       0       20          200     800         80
PeGi 255/3/28   Up      1       0       20          200     800         80
PeGi 255/3/29   Up      1       0       20          200     800         80
PeGi 255/3/30   Up      1       0       20          200     800         80
PeGi 255/3/31   Up      1       0       20          200     800         80
PeGi 255/3/32   Up      1       0       20          200     800         80
PeGi 255/3/33   Up      1       0       20          200     800         80
PeGi 255/3/34   Up      1       0       20          200     800         80
PeGi 255/3/35   Up      1       0       20          200     800         80
PeGi 255/3/36   Up      1       0       20          200     800         80
PeGi 255/3/37   Up      1       0       20          200     800         80
PeGi 255/3/38   Up      1       0       20          200     800         80
PeGi 255/3/39   Up      0       0       20          200     800         80
PeGi 255/3/40   Up      1       0       20          200     800         80
PeGi 255/3/41   Up      0       0       20          200     800         80
PeGi 255/3/42   Up      0       0       20          200     800         80
PeGi 255/3/43   Up      1       0       20          200     800         80
PeGi 255/3/44   Up      1       0       20          200     800         80
PeGi 255/3/45   Up      1       0       20          200     800         80
PeGi 255/3/46   Up      0       0       20          200     800         80
PeGi 255/3/47   Up      0       0       20          200     800         80
PeGi 255/3/48   Up      0       0       20          200     800         80
```

Example show interfaces dampening detail

```
Dell# show interfaces dampening detail

Interface                              : TenGigabitEthernet 2/0
Operation state                        : down
Suppression state                      : Up
Flap count                             : 0
Penalty                                : 0
Half life                              : 5
Reuse threshold                        : 200
Suppression threshold                  : 250
Max suppression time                   : 300
Time since last suppressed             : 0
Time remaining to change state to up : 0
```

Related Commands

- dampening — configures dampening on an interface.
- show interfaces — displays information on a specific physical interface or virtual interface.

- show interfaces configured — displays any interface with a non-default configuration.

show interfaces phy

Display auto-negotiation and link partner information.

C9000 Series

Syntax

```
show interfaces gigabitethernet slot/port phy
```

Parameters

gigabitethernet	Enter the keyword `gigabitethernet` then the slot/port information.
tengigabitethernet	Enter the keyword `tengigabitethernet` then the slot or port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.
6.5.4.0	Introduced on the E-Series.

Usage Information

The following describes the `show interfaces tengigabitethernet` command following example.

Mode Control	Indicates if `auto negotiation` is enabled. If so, indicates the selected speed and duplex.
Mode Status	Displays auto negotiation fault information. When the interface completes auto negotiation successfully, the `autoNegComplete` field and the `linkstatus` field read "True."
AutoNegotiation Advertise	Displays the control words the local interface advertises during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control the local interface supports.
AutoNegotiation Remote Partner's Ability	Displays the control words the remote interface advertises during negotiation. Duplex is either half or full. Asym- and Sym Pause is the types of flow control the remote interface supports.

AutoNegotiation Expansion	ParallelDetectionFault is the handshaking scheme in which the link partner continuously transmit an “idle” data packet using the Fast Ethernet MLT-3 waveform. Equipment that does not support auto-negotiation must be configured to exactly match the mode of operation as the link partner or else no link can be established.
1000Base-T Control	1000Base-T requires auto-negotiation. The IEEE Ethernet standard does not support setting a speed to 1000 Mbps with the `speed` command without auto-negotiation. E-Series line cards support both full-duplex and half-duplex 1000BaseT.
Phy Specific Control	Values are: • 0 - Manual MDI • 1 - Manual MDIX • 2 - N/A • 3 - Auto MDI/MDIX
Phy Specific Status	Displays PHY-specific status information. Cable length represents a rough estimate in meters: • 0 - < 50 meters • 1 - 50 - 80 meters • 2 - 80 - 110 meters • 3 - 110 - 140 meters • 4 - 140 meters Link Status: Up or Down Speed: • Auto • 1000MB • 100MB • 10MB

Example

```
Dell#show int tengigabitethernet 1/0 phy
Mode Control:
  SpeedSelection:         10b
  AutoNeg:                ON
  Loopback:               False
  PowerDown:              False
  Isolate:                False
  DuplexMode:             Full
Mode Status:
  AutoNegComplete:        False
  RemoteFault:            False
  LinkStatus:             False
  JabberDetect:           False
AutoNegotation Advertise:
  100MegFullDplx:         True
  100MegHalfDplx:         True
  10MegFullDplx:          False
  10MegHalfDplx:          True
  Asym Pause:             False
  Sym Pause:              False
AutoNegotiation Remote Partner's Ability:
  100MegFullDplx:         False
  100MegHalfDplx:         False
  10MegFullDplx:          False
  10MegHalfDplx:          False
```

```
  Asym Pause:             False
  Sym Pause:              False
AutoNegotiation Expansion:
  ParallelDetectionFault: False
...
```

Example (port range)

```
Dell#show interfaces gigabitethernet 1/1-1/2 phy

Interface Name                 :GigabitEthernet 1/1
Mode Control
    SpeedSelection            : 10b
    AutoNeg                   : ON
    Loopback                  : False
    PowerDown                 : True
    Isolate                   : False
    DuplexMode                : Full

Mode Status
    AutoNegComplete           : False
    RemoteFault               : False
    LinkStatus                : Down
    JabberDetect              : False

AutoNegotiation Advertise
    100MegFullDplx            : True
    100MegHalfDplx            : False
    10MegFullDplx             : True
    10MegHalfDplx             : False
    Asym Pause                : False
    Sym Pause                 : False

AutoNegotiation Remote Partner's Ability
    100MegFullDplx            : False
    100MegHalfDplx            : False
    10MegFullDplx             : False
    10MegHalfDplx             : False
    Asym Pause                : False
    Sym Pause                 : False

AutoNegotiation Expansion
    ParallelDetectionFault    : False

1000Base-T Control
    MasterSlave_Mode          : Auto
    1000MegFullDplx           : True
    1000MegHalfDplx           : False

1000Base-T Status
    Master/Slave Fault        : No
    Master/Slave              : Slave
    Local RX OK               : False
    Remote RX OK              : False
    Link Partner 1G FD        : False
    Link Partner 1G HD        : False
    Idle Err Cnt              : 0

PHY Extended Control
    MDI Crossover_mode        : Enabled

Interface Name                 :GigabitEthernet 1/2
Mode Control
    SpeedSelection            : 10b
    AutoNeg                   : ON
    Loopback                  : False
    PowerDown                 : True
    Isolate                   : False
    DuplexMode                : Full
```

```
Mode Status
    AutoNegComplete           : False
    RemoteFault               : False
    LinkStatus                : Down
    JabberDetect              : False

AutoNegotiation Advertise
    100MegFullDplx            : True
    100MegHalfDplx            : False
    10MegFullDplx             : True
    10MegHalfDplx             : False
    Asym Pause                : False
    Sym Pause                 : False

AutoNegotiation Remote Partner's Ability
    100MegFullDplx            : False
    100MegHalfDplx            : False
    10MegFullDplx             : False
    10MegHalfDplx             : False
    Asym Pause                : False
    Sym Pause                 : False

AutoNegotiation Expansion
    ParallelDetectionFault    : False

1000Base-T Control
    MasterSlave_Mode          : Auto
    1000MegFullDplx           : True
    1000MegHalfDplx           : False

1000Base-T Status
    Master/Slave Fault        : No
    Master/Slave              : Slave
    Local RX OK               : False
    Remote RX OK              : False
    Link Partner 1G FD        : False
    Link Partner 1G HD        : False
    Idle Err Cnt              : 0

PHY Extended Control
    MDI Crossover_mode        : Enabled
```

Example

Related Commands show interfaces — displays information on a specific physical interface or virtual interface.

show interfaces status

To display status information on a specific interface only, display a summary of interface information or specify a line card slot and interface.

C9000 Series

Syntax `show interfaces [interface | linecard slot-number] status`

Parameters

interface (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port (ports or port-range) information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port (ports or port-range) information.

- For a Loopback interface, enter the keyword `loopback` then the slot/port information. The range is from 0 to 16383.
- For a Port-Channel interface, enter the keyword `port-channel` then the number. The range is from 0 to 128.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

NOTE: The peGigE or peTenGigE interface option is only visible when the feature extended bridge is enabled.

linecard *slot-number*	(OPTIONAL) Enter the keyword `linecard` then the slot number. The slot ID is from 0 to 11.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

Usage Information

To view the show output for multiple ports of a specified slot at a time, you can specify any random port number or a range of ports, or a combination of both.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces status FortyGigE 1/0-4,7,9-11`. To enter any random number of ports, you can enter a comma-separated string of port numbers, for example `show interfaces status FortyGigE 1/0/1,9,11`

NOTE: The port-range option is only available for 1 Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, Fast Ethernet, FC, Port Channel, and VLAN interfaces.

```
Dell#sho interfaces status | no-more
Port         Description  Status Speed     Duplex Vlan
Fo 0/0                    Down   40000 Mbit Auto   --
Fo 0/4                    Down   40000 Mbit Auto   --
Fo 0/8                    Down   40000 Mbit Auto   --
Fo 0/12                   Down   40000 Mbit Auto   --
Fo 0/16                   Down   40000 Mbit Auto   --
Fo 0/20                   Down   40000 Mbit Auto   --
Te 2/0                    Down   Auto      Auto   --
Te 2/1                    Down   Auto      Auto   --
Te 2/2                    Down   Auto      Auto   --
Te 2/3                    Down   Auto      Auto   --
Te 2/4                    Down   Auto      Auto   --
Te 2/5                    Down   Auto      Auto   --
Te 2/6                    Down   Auto      Auto   --
Te 2/7                    Down   Auto      Auto   --
Te 2/8                    Down   Auto      Auto   --
Te 2/9                    Down   Auto      Auto   --
Te 2/10                   Down   Auto      Auto   --
Te 2/11                   Down   Auto      Auto   --
Te 2/12                   Down   Auto      Auto   --
Te 2/13                   Down   Auto      Auto   --
Te 2/14                   Down   Auto      Auto   --
Te 2/15                   Down   Auto      Auto   --
Te 2/16                   Down   Auto      Auto   --
Te 2/17                   Down   Auto      Auto   --
Te 2/18                   Down   Auto      Auto   --
Te 2/19                   Down   Auto      Auto   --
Te 2/20                   Down   Auto      Auto   --
Te 2/21                   Down   Auto      Auto   --
Te 2/22                   Down   Auto      Auto   --
Te 2/23                   Down   Auto      Auto   --
Fo 5/0                    Down   40000 Mbit Auto   --
Fo 5/4                    Down   40000 Mbit Auto   --
Fo 5/8                    Down   40000 Mbit Auto   --
Fo 5/12                   Down   40000 Mbit Auto   --
Fo 5/16                   Down   40000 Mbit Auto   --
Fo 5/20                   Down   40000 Mbit Auto   --
Te 6/0                    Down   Auto      Auto   --
Te 6/1                    Down   Auto      Auto   --
Te 6/2                    Down   Auto      Auto   --
Te 6/3                    Down   Auto      Auto   --
Te 6/4                    Down   Auto      Auto   --
Te 6/5                    Down   Auto      Auto   --
Te 6/6                    Down   Auto      Auto   --
Te 6/7                    Down   Auto      Auto   --
Te 6/8                    Down   Auto      Auto   --
Te 6/9                    Down   Auto      Auto   --
Te 6/10                   Down   Auto      Auto   --
Te 6/11                   Down   Auto      Auto   --
Te 6/12                   Down   Auto      Auto   --
Te 6/13                   Down   Auto      Auto   --
Te 6/14                   Down   Auto      Auto   --
Te 6/15                   Down   Auto      Auto   --
Te 6/16                   Down   Auto      Auto   --
Te 6/17                   Down   Auto      Auto   --
Te 6/18                   Down   Auto      Auto   --
Te 6/19                   Down   Auto      Auto   --
Te 6/20                   Down   Auto      Auto   --
Te 6/21                   Up     10000 Mbit Full   --
Te 6/22                   Down   Auto      Auto   --
Te 6/23                   Up     10000 Mbit Full   --
Fo 9/0                    Down   40000 Mbit Auto   --
Fo 9/4                    Down   40000 Mbit Auto   --
Fo 9/8                    Down   40000 Mbit Auto   --
```

```
Fo 9/12                  Down   40000 Mbit Auto   --
Fo 9/16                  Down   40000 Mbit Auto   --
Fo 9/20                  Down   40000 Mbit Auto   --
Te 10/0                  Down   Auto      Auto   --
Te 10/1                  Down   Auto      Auto   --
Te 10/2                  Down   Auto      Auto   --
Te 10/3                  Down   Auto      Auto   1
Te 11/0                  Down   Auto      Auto   --
Te 11/1                  Down   Auto      Auto   --
Te 11/2                  Down   Auto      Auto   --
Te 11/3                  Down   Auto      Auto   --
PeGi 255/1/1             Up     1000 Mbit Full   --
PeGi 255/1/2             Up     1000 Mbit Full   --
PeGi 255/1/3             Up     1000 Mbit Full   --
PeGi 255/1/4             Up     1000 Mbit Full   --
PeGi 255/1/5             Up     1000 Mbit Full   --
PeGi 255/1/6             Up     1000 Mbit Full   --
PeGi 255/1/7             Up     1000 Mbit Full   --
PeGi 255/1/8             Up     1000 Mbit Full   --
PeGi 255/1/9             Up     1000 Mbit Full   --
PeGi 255/1/10             Up     1000 Mbit Full   --
PeGi 255/1/11             Up     1000 Mbit Full   --
PeGi 255/1/12             Up     1000 Mbit Full   --
PeGi 255/1/13             Up     1000 Mbit Full   --
PeGi 255/1/14             Up     1000 Mbit Full   --
PeGi 255/1/15             Up     1000 Mbit Full   --
PeGi 255/1/16             Up     1000 Mbit Full   --
PeGi 255/1/17             Up     1000 Mbit Full   --
PeGi 255/1/18             Up     1000 Mbit Full   --
PeGi 255/1/19             Up     1000 Mbit Full   --
PeGi 255/1/20             Up     1000 Mbit Full   --
PeGi 255/1/21             Up     1000 Mbit Full   --
PeGi 255/1/22             Up     1000 Mbit Full   --
PeGi 255/1/23             Up     1000 Mbit Full   --
PeGi 255/1/24             Up     1000 Mbit Full   --
PeGi 255/1/25             Up     1000 Mbit Full   --
PeGi 255/1/26             Up     1000 Mbit Full   --
PeGi 255/1/27             Up     1000 Mbit Full   --
PeGi 255/1/28             Up     1000 Mbit Full   --
PeGi 255/1/29             Up     1000 Mbit Full   --
PeGi 255/1/30             Up     1000 Mbit Full   --
PeGi 255/1/31             Up     1000 Mbit Full   --
PeGi 255/1/32             Up     1000 Mbit Full   --
PeGi 255/1/33             Up     1000 Mbit Full   --
PeGi 255/1/34             Up     1000 Mbit Full   --
PeGi 255/1/35             Up     1000 Mbit Full   --
PeGi 255/1/36             Up     1000 Mbit Full   --
PeGi 255/1/37             Up     1000 Mbit Full   --
PeGi 255/1/38             Up     1000 Mbit Full   --
PeGi 255/1/39             Up     1000 Mbit Full   --
PeGi 255/1/40             Up     1000 Mbit Full   --
PeGi 255/1/41             Up     1000 Mbit Full   --
PeGi 255/1/42             Up     1000 Mbit Full   --
PeGi 255/1/43             Up     1000 Mbit Full   --
PeGi 255/1/44             Up     1000 Mbit Full   --
PeGi 255/1/45             Up     1000 Mbit Full   --
PeGi 255/1/46             Up     1000 Mbit Full   111
PeGi 255/1/47             Up     1000 Mbit Full   111
PeGi 255/1/48             Up     1000 Mbit Full   111
PeGi 255/2/1              Up     1000 Mbit Full   111
PeGi 255/2/2              Up     1000 Mbit Full   --
PeGi 255/2/3              Up     1000 Mbit Full   --
PeGi 255/2/4              Up     1000 Mbit Full   --
PeGi 255/2/5              Up     1000 Mbit Full   --
PeGi 255/2/6              Up     1000 Mbit Full   --
PeGi 255/2/7              Up     1000 Mbit Full   --
PeGi 255/2/8              Up     1000 Mbit Full   --
PeGi 255/2/9              Up     1000 Mbit Full   --
PeGi 255/2/10             Up     1000 Mbit Full   --
```

```
PeGi 255/2/11               Up     1000 Mbit Full   --
PeGi 255/2/12               Up     1000 Mbit Full   --
PeGi 255/2/13               Up     1000 Mbit Full   --
PeGi 255/2/14               Up     1000 Mbit Full   --
PeGi 255/2/15               Up     1000 Mbit Full   --
PeGi 255/2/16               Up     1000 Mbit Full   --
PeGi 255/2/17               Up     1000 Mbit Full   --
PeGi 255/2/18               Up     1000 Mbit Full   --
PeGi 255/2/19               Up     1000 Mbit Full   --
PeGi 255/2/20               Up     1000 Mbit Full   --
PeGi 255/2/21               Up     1000 Mbit Full   --
PeGi 255/2/22               Up     1000 Mbit Full   --
PeGi 255/2/23               Up     1000 Mbit Full   --
PeGi 255/2/24               Up     1000 Mbit Full   --
PeGi 255/2/25               Up     1000 Mbit Full   --
PeGi 255/2/26               Up     1000 Mbit Full   --
PeGi 255/2/27               Up     1000 Mbit Full   --
PeGi 255/2/28               Up     1000 Mbit Full   --
PeGi 255/2/29               Up     1000 Mbit Full   --
PeGi 255/2/30               Up     1000 Mbit Full   --
PeGi 255/2/31               Up     1000 Mbit Full   --
PeGi 255/2/32               Up     1000 Mbit Full   --
PeGi 255/2/33               Up     1000 Mbit Full   --
PeGi 255/2/34               Up     1000 Mbit Full   --
PeGi 255/2/35               Up     1000 Mbit Full   --
PeGi 255/2/36               Up     1000 Mbit Full   --
PeGi 255/2/37               Up     1000 Mbit Full   --
PeGi 255/2/38               Up     1000 Mbit Full   --
PeGi 255/2/39               Up     1000 Mbit Full   --
PeGi 255/2/40               Up     1000 Mbit Full   --
PeGi 255/2/41               Up     1000 Mbit Full   --
PeGi 255/2/42               Up     1000 Mbit Full   --
PeGi 255/2/43               Up     1000 Mbit Full   --
PeGi 255/2/44               Up     1000 Mbit Full   --
PeGi 255/2/45               Up     1000 Mbit Full   --
PeGi 255/2/46               Down   Auto       Auto   --
PeGi 255/2/47               Down   Auto       Auto   --
PeGi 255/2/48               Down   Auto       Auto   --
PeGi 255/3/1                Up     1000 Mbit Full   --
PeGi 255/3/2                Up     1000 Mbit Full   --
PeGi 255/3/3                Up     1000 Mbit Full   --
PeGi 255/3/4                Up     1000 Mbit Full   --
PeGi 255/3/5                Up     1000 Mbit Full   --
PeGi 255/3/6                Up     1000 Mbit Full   --
PeGi 255/3/7                Up     1000 Mbit Full   --
PeGi 255/3/8                Up     1000 Mbit Full   --
PeGi 255/3/9                Up     1000 Mbit Full   --
PeGi 255/3/10               Up     1000 Mbit Full   --
PeGi 255/3/11               Up     1000 Mbit Full   --
PeGi 255/3/12               Up     1000 Mbit Full   --
PeGi 255/3/13               Up     1000 Mbit Full   --
PeGi 255/3/14               Up     1000 Mbit Full   --
PeGi 255/3/15               Up     1000 Mbit Full   --
PeGi 255/3/16               Up     1000 Mbit Full   --
PeGi 255/3/17               Up     1000 Mbit Full   --
PeGi 255/3/18               Up     1000 Mbit Full   --
PeGi 255/3/19               Up     1000 Mbit Full   --
PeGi 255/3/20               Up     1000 Mbit Full   --
PeGi 255/3/21               Up     1000 Mbit Full   --
PeGi 255/3/22               Up     1000 Mbit Full   --
PeGi 255/3/23               Up     1000 Mbit Full   --
PeGi 255/3/24               Up     1000 Mbit Full   --
PeGi 255/3/25               Up     1000 Mbit Full   --
PeGi 255/3/26               Up     1000 Mbit Full   --
PeGi 255/3/27               Up     1000 Mbit Full   --
PeGi 255/3/28               Up     1000 Mbit Full   --
PeGi 255/3/29               Up     1000 Mbit Full   --
PeGi 255/3/30               Up     1000 Mbit Full   --
PeGi 255/3/31               Up     1000 Mbit Full   --
```

```
PeGi 255/3/32              Up     1000 Mbit Full   --
PeGi 255/3/33              Up     1000 Mbit Full   --
PeGi 255/3/34              Up     1000 Mbit Full   --
PeGi 255/3/35              Up     1000 Mbit Full   --
PeGi 255/3/36              Up     1000 Mbit Full   --
PeGi 255/3/37              Up     1000 Mbit Full   --
PeGi 255/3/38              Up     1000 Mbit Full   --
PeGi 255/3/39              Down   Auto      Auto   --
PeGi 255/3/40              Up     1000 Mbit Full   --
PeGi 255/3/41              Down   Auto      Auto   --
PeGi 255/3/42              Down   Auto      Auto   --
PeGi 255/3/43              Up     1000 Mbit Full   --
PeGi 255/3/44              Up     1000 Mbit Full   --
PeGi 255/3/45              Up     1000 Mbit Full   --
PeGi 255/3/46              Down   Auto      Auto   --
PeGi 255/3/47              Up     1000 Mbit Full   111
PeGi 255/3/48              Up     1000 Mbit Full   111
```

Related Commands show interfaces — displays information on a specific physical interface or virtual interface.

show interfaces switchport

Display only virtual and physical interfaces in Layer 2 mode. This command displays the Layer 2 mode interfaces' IEEE 802.1Q tag status and VLAN membership.

C9000 Series

Syntax `show interfaces switchport [interface] [linecard slot-id]`

Parameters

interface (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port (ports or port-range) information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port (ports or port-range) information.
- Enter the keyword `backup` to view the backup interface for this interface.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number*range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

NOTE: The peGigE or peTenGigE interface option is only visible when the feature extended bridge is enabled.

linecard *slot-id* Enter the `linecard slot-id` parameters to specify the switch ports on a line card. The range of slot IDs is from 0 to 11.

Command Modes

- EXEC

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Added support for 4093 VLANs on E-Series ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Support added for hybrid port/native VLAN, introduced on the S Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

To view the switchport information for multiple ports of a specified slot, you can specify any random port number or a range of ports, or a combination of both.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces tengigabitethernet 10/0-1 switchport`

NOTE: The multiple port range value is supported only for the Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, Fast Ethernet, FC, Port Channel, and VLAN interfaces.

The following describes the `show interfaces switchport` command for the following example.

Items	Description
Name	Displays the interface's type, slot, and port number.
802.1QTagged	Displays whether if the VLAN tagged ("True"), untagged ("False"), or hybrid ("Hybrid"), which supports both untagged and tagged VLANs by port 13/0.
Vlan membership	Lists the VLANs to which the interface is a member.

Example

```
Dell#show interfaces switchport

Codes:  U - Untagged, T - Tagged
        x - Dot1x untagged, X - Dot1x tagged
        G - GVRP tagged, M - Trunk
        i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT
tagged

Name: TenGigabitEthernet 10/3
802.1QTagged: False
Vlan membership:
Q       Vlans
U       1
```

```
Name: peGigE 255/1/36 (Port-channel 111)
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/1/37 (Port-channel 111)
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/1/46
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/1/47
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/2/1
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/2/2
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/2/38 (Port-channel 111)
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/2/39 (Port-channel 111)
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/3/1
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/3/40 (Port-channel 111)
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111
```

```
Name: peGigE 255/3/45 (Port-channel 111)
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: peGigE 255/3/47
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111


Name: Port-channel 22
802.1QTagged: True
Vlan membership:
Q       Vlans
T       222


Name: Port-channel 111
802.1QTagged: True
Vlan membership:
Q       Vlans
T       111
```

Example (port range)

```
Dell#show interfaces switchport tengigabitethernet 10/0-1

Codes:  U - Untagged, T - Tagged
        x - Dot1x untagged, X - Dot1x tagged
        G - GVRP tagged, M - Trunk
        i - Internal untagged, I-Internal tagged, v-VLT untagged, V-VLT tagged

Name: TenGigabitEthernet 10/0
802.1QTagged: False
Vlan membership:
Q       Vlans
U       1



Name: TenGigabitEthernet 10/1
802.1QTagged: False
Vlan membership:
Q       Vlans
U       1
```

Related Commands

- interface — configures a physical interface on the switch.
- show ip interface — displays Layer 3 information about the interfaces.
- show interfaces — displays information on a specific physical interface or virtual interface.
- show interfaces transceiver — displays the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

show interfaces transceiver

Display the physical status and operational status of an installed transceiver. The output also displays the transceiver's serial number.

C9000 Series

Syntax

```
show interfaces [tengigabitethernet slot/port | fortyGigE slot/port | peGigE pe-id/stack-unit/port | peTenGigE pe-id/stack-unit/port] transceiver
```

Parameters

tengigabitethernet	For a 10G interface, enter the keyword `tengigabitethernet` then the slot/port (ports or port range) information.
fortyGigE	For a 40G interface, enter the keyword `fortyGigE` then the slot/port (ports or port-range)information.
peGigE	For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48. **NOTE: The peGigE or peTenGigE option is only visible when the feature extended bridge feature is enabled.**
peTenGigE	For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Output augmented with diagnostic data for pluggable media.
7.7.1.0	Removed three fields in the output: Vendor Name, Vendor OUI, and Vendor PN.

Version	Description
7.6.1.0	Introduced on the C-Series and S-Series.
6.5.4.0	Introduced on the E-Series.

Usage Information The following describes the `show interfaces transceiver` command shown in the following example.

Line	Description
Rx Power measurement type	Output depends on the vendor, typically either “Average” or “OMA” (Receiver optical modulation amplitude).
Temp High Alarm threshold	Factory-defined setting, typically in Centigrade. Value differs between SFPs and SFP+.
Voltage High Alarm threshold	Displays the interface index number that SNMP uses to identify the interface.
Bias High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power Low Alarm threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Bias High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
RX Power High Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temp Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Voltage Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.

Line	Description
Bias Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
TX Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Power Low Warning threshold	Factory-defined setting. Value can differ between SFP and SFP+.
Temperature	Current temperature of the SFPs. If this temperature crosses Temp High alarm/warning thresholds, the temperature high alarm/warning flag is set to true.
Voltage	Current voltage of the SFPs. If this voltage crosses voltage high alarm/warning thresholds, the voltage high alarm/warning flag is set to true.
Tx Bias Current	Present transmission (Tx) bias current of the SFP. If this crosses bias high alarm/warning thresholds, the TX bias high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the TX bias low alarm/warning flag is set to true.
Tx Power	Present Tx power of the SFP. If this crosses Tx power alarm/warning thresholds, the Tx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the Tx power low alarm/ warning flag is set to true.
Rx Power	Present receiving (Rx) power of the SFP. This value is either average Rx power or OMA. This depends on the Rx Power measurement type displayed above. If this crosses Rx power alarm/warning thresholds, the Rx power high alarm/warning flag is set to true. If it falls below the low alarm/warning thresholds, the Rx power low alarm/warning flag is set to true.
Data Ready state Bar	This field indicates that the transceiver has achieved power up and data is ready. This is set to true if data is ready to be sent and set to false if data is being transmitted.
Rx LOS state	This is the digital state of the Rx_LOS output pin. This is set to true if the operating status is down.
Tx Fault state	This is the digital state of the Tx Fault output pin.
Rate Select state	This is the digital state of the SFP rate_select input pin.
RS state	This is the reserved digital state of the pin AS(1) per SFF-8079 and RS(1) per SFF-8431.
Tx Disable state	If the admin status of the port is down, then this flag is set to true.
Temperature High Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.
Voltage High Alarm Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Tx Bias High Alarm Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power High Alarm Flag	This can be either true or false, depending on the Current Tx bias power value displayed above.
Rx Power High Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature Low Alarm Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Alarm Flag	This can be either true or false, depending on the Current voltage value displayed above.

Line	Description
Tx Bias Low Alarm Flag	This can be either true or false, depending on the Tx bias current value displayed above.
Tx Power Low Alarm Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Alarm Flag	This can be either true or false, depending on the Current Rx power value displayed above.
Temperature High Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage High Warning Flag	This can be either true or false, depending on the Current Voltage value displayed above.
Tx Bias High Warning Flag	This can be either true or false, depending on the Tx bias current value displayed above.
Tx Power High Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power High Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Temperature Low Warning Flag	This can be either true or false, depending on the Current Temperature value displayed above.
Voltage Low Warning Flag	This can be either true or false, depending on the Current Voltage value displayed above.
Tx Bias Low Warning Flag	This can be either true or false, depending on the present Tx bias current value displayed above.
Tx Power Low Warning Flag	This can be either true or false, depending on the Current Tx power value displayed above.
Rx Power Low Warning Flag	This can be either true or false, depending on the Current Rx power value displayed above.

To view the transceiver information for multiple ports of a specified slot, you can specify any random port number or a range of ports, or a combination of both.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces tengigabitethernet 10/0-2 transceiver`

Example

```
Dell# show interfaces tengigabitethernet 1/0 transceiver
SFP is present.

SFP 0 Serial Base ID fields
SFP 0 Id                  = 0x03
SFP 0 Ext Id              = 0x04
SFP 0 Connector           = 0x07
SFP 0 Transciever Code = 0x00 0x00 0x00 0x01 0x20 0x40 0x0c 0x05
SFP 0 Encoding            = 0x01
SFP 0 BR Nominal          = 0x15
SFP 0 Length(9um) Km      = 0x00
SFP 0 Length(9um) 100m    = 0x00
SFP 0 Length(50um) 10m    = 0x1e
SFP 0 Length(62.5um) 10m  = 0x0f
SFP 0 Length(Copper) 10m  = 0x00
SFP 0 Vendor Rev          = A
SFP 0 Laser Wavelength    = 850 nm
SFP 0 CheckCodeBase       = 0x66
```

```
SFP 0 Serial Extended ID fields
SFP 0 Options             = 0x00 0x12
SFP 0 BR max= 0
SFP 0 BR min= 0
SFP 0 Vendor SN= P5N1ACE
SFP 0 Datecode            = 040528
SFP 0 CheckCodeExt        = 0x5b

SFP 1 Diagnostic Information
==================================
SFP 1 Rx Power measurement type     = Average
==================================
SFP 1 Temp High Alarm threshold       = 95.000C
SFP 1 Voltage High Alarm threshold    = 3.900V
SFP 1 Bias High Alarm threshold       = 17.000mA
SFP 1 TX Power High Alarm threshold   = 0.631mW
SFP 1 RX Power High Alarm threshold   = 1.259mW
SFP 1 Temp Low Alarm threshold        = -25.000C
SFP 1 Voltage Low Alarm threshold     = 2.700V
SFP 1 Bias Low Alarm threshold        = 1.000mA
SFP 1 TX Power Low Alarm threshold    = 0.067mW
SFP 1 RX Power Low Alarm threshold    = 0.010mW
==================================
SFP 1 Temp High Warning threshold     = 90.000C
SFP 1 Voltage High Warning threshold  = 3.700V
SFP 1 Bias High Warning threshold     = 14.000mA
SFP 1 TX Power High Warning threshold = 0.631mW
SFP 1 RX Power High Warning threshold = 0.794mW
SFP 1 Temp Low Warning threshold      = -20.000C
SFP 1 Voltage Low Warning threshold   = 2.900V
SFP 1 Bias Low Warning threshold      = 2.000mA
SFP 1 TX Power Low Warning threshold  = 0.079mW
SFP 1 RX Power Low Warning threshold  = 0.016mW
==================================
SFP 1 Temperature                     = 39.930C
SFP 1 Voltage                         = 3.293V
SFP 1 Tx Bias Current                 = 6.894mA
SFP 1 Tx Power                        = 0.328mW
SFP 1 Rx Power                        = 0.000mW
==================================
SFP 1 Data Ready state Bar            = False
SFP 1 Rx LOS state                    = True
SFP 1 Tx Fault state                  = False
SFP 1 Rate Select state               = False
SFP 1 RS state                        = False
SFP 1 Tx Disable state                = False
==================================
SFP 1 Temperature High Alarm Flag     = False
SFP 1 Voltage High Alarm Flag         = False
SFP 1 Tx Bias High Alarm Flag         = False
SFP 1 Tx Power High Alarm Flag        = False
SFP 1 Rx Power High Alarm Flag        = False
SFP 1 Temperature Low Alarm Flag      = False
SFP 1 Voltage Low Alarm Flag          = False
SFP 1 Tx Bias Low Alarm Flag          = False
SFP 1 Tx Power Low Alarm Flag         = False
SFP 1 Rx Power Low Alarm Flag         = True
==================================
!-------output truncated -------------------------!
```

Example-tengigabitethernet (port-range)

```
Dell#show interfaces tengigabitethernet 10/0-2 transceiver

Interface Name                 :TenGigabitEthernet 10/0
SFP is present
SFP+ 0 Serial Base ID fields
SFP+ 0 Id                       = 0x03
SFP+ 0 Ext Id                   = 0x04
SFP+ 0 Connector                = 0x07
```

```
SFP+ 0 Transceiver Code         = 0x10 0x00 0x00 0x00 0x00 0x00 0x00 0x00
SFP+ 0 Encoding                 = 0x06
SFP+ 0 BR Nominal               = 0x67
SFP+ 0 Length(SFM)    Km        = 0x00
SFP+ 0 Length(OM3)    2m        = 0x00
SFP+ 0 Length(OM2)    1m        = 0x08
SFP+ 0 Length(OM1)    1m        = 0x03
SFP+ 0 Length(Copper) 1m        = 0x00
SFP+ 0 Vendor Rev               = A
SFP+ 0 Laser Wavelength         = 850 nm
SFP+ 0 CheckCodeBase            = 0x9e
SFP+ 0 Serial Extended ID fields
SFP+ 0 Options                  = 0x00 0x1a
SFP+ 0 BR max                   = 0
SFP+ 0 BR min                   = 0
SFP+ 0 Vendor SN                = AQM1AHB
SFP+ 0 Datecode                 = 131122
SFP+ 0 CheckCodeExt             = 0xda

SFP+ 0 Diagnostic Information
=================================
SFP+ 0 Rx Power measurement type        = Average
=================================
SFP+ 0 Temp High Alarm threshold        = 78.000C
SFP+ 0 Voltage High Alarm threshold     = 3.700V
SFP+ 0 Bias High Alarm threshold        = 13.200mA
SFP+ 0 TX Power High Alarm threshold    = 1.000mW
SFP+ 0 RX Power High Alarm threshold    = 1.000mW
SFP+ 0 Temp Low Alarm threshold         = -13.000C
SFP+ 0 Voltage Low Alarm threshold      = 2.900V
SFP+ 0 Bias Low Alarm threshold         = 4.000mA
SFP+ 0 TX Power Low Alarm threshold     = 0.251mW
SFP+ 0 RX Power Low Alarm threshold     = 0.010mW
=================================
SFP+ 0 Temp High Warning threshold      = 73.000C
SFP+ 0 Voltage High Warning threshold   = 3.600V
SFP+ 0 Bias High Warning threshold      = 12.600mA
SFP+ 0 TX Power High Warning threshold  = 0.794mW
SFP+ 0 RX Power High Warning threshold  = 0.794mW
SFP+ 0 Temp Low Warning threshold       = -8.000C
SFP+ 0 Voltage Low Warning threshold    = 3.000V
SFP+ 0 Bias Low Warning threshold       = 5.000mA
SFP+ 0 TX Power Low Warning threshold   = 0.316mW
SFP+ 0 RX Power Low Warning threshold   = 0.016mW
=================================
SFP+ 0 Temperature                      = 33.871C
SFP+ 0 Voltage                          = 3.277V
SFP+ 0 Tx Bias Current                  = 7.634mA
SFP+ 0 Tx Power                         = 0.562mW
SFP+ 0 Rx Power                         = 0.579mW
=================================
SFP+ 0 Data Ready state Bar             = False
SFP+ 0 Rx LOS state                     = False
SFP+ 0 Tx Fault state                   = False
SFP+ 0 Rate Select state                = True
SFP+ 0 RS state                         = True
SFP+ 0 Tx Disable state                 = False
=================================
SFP+ 0 Temperature High Alarm Flag      = False
SFP+ 0 Voltage High Alarm Flag          = False
SFP+ 0 Tx Bias High Alarm Flag          = False
SFP+ 0 Tx Power High Alarm Flag         = False
SFP+ 0 Rx Power High Alarm Flag         = False
SFP+ 0 Temperature Low Alarm Flag       = False
SFP+ 0 Voltage Low Alarm Flag           = False
SFP+ 0 Tx Bias Low Alarm Flag           = False
SFP+ 0 Tx Power Low Alarm Flag          = False
SFP+ 0 Rx Power Low Alarm Flag          = False
=================================
```

```
SFP+ 0 Temperature High Warning Flag    = False
SFP+ 0 Voltage High Warning Flag        = False
SFP+ 0 Tx Bias High Warning Flag        = False
SFP+ 0 Tx Power High Warning Flag       = False
SFP+ 0 Rx Power High Warning Flag       = False
SFP+ 0 Temperature Low Warning Flag     = False
SFP+ 0 Voltage Low Warning Flag         = False
SFP+ 0 Tx Bias Low Warning Flag         = False
SFP+ 0 Tx Power Low Warning Flag        = False
SFP+ 0 Rx Power Low Warning Flag        = False


Interface Name                 :TenGigabitEthernet 10/1
SFP is present
SFP+ 1 Serial Base ID fields
SFP+ 1 Id                       = 0x03
SFP+ 1 Ext Id                   = 0x04
SFP+ 1 Connector                = 0x07
SFP+ 1 Transceiver Code         = 0x10 0x00 0x00 0x00 0x00 0x00 0x00 0x00
SFP+ 1 Encoding                 = 0x06
SFP+ 1 BR Nominal               = 0x67
SFP+ 1 Length(SFM)    Km        = 0x00
SFP+ 1 Length(OM3)    2m        = 0x00
SFP+ 1 Length(OM2)    1m        = 0x08
SFP+ 1 Length(OM1)    1m        = 0x03
SFP+ 1 Length(Copper) 1m        = 0x00
SFP+ 1 Vendor Rev               = 1
SFP+ 1 Laser Wavelength         = 850 nm
SFP+ 1 CheckCodeBase            = 0xf9
SFP+ 1 Serial Extended ID fields
SFP+ 1 Options                  = 0x00 0x1a
SFP+ 1 BR max                   = 0
SFP+ 1 BR min                   = 0
SFP+ 1 Vendor SN                = CD07FM0R0
SFP+ 1 Datecode                 = 130216
SFP+ 1 CheckCodeExt             = 0xf5

SFP+ 1 Diagnostic Information
==================================
SFP+ 1 Rx Power measurement type        = Average
==================================
SFP+ 1 Temp High Alarm threshold        = 80.000C
SFP+ 1 Voltage High Alarm threshold     = 3.700V
SFP+ 1 Bias High Alarm threshold        = 10.000mA
SFP+ 1 TX Power High Alarm threshold    = 0.794mW
SFP+ 1 RX Power High Alarm threshold    = 1.413mW
SFP+ 1 Temp Low Alarm threshold         = -10.000C
SFP+ 1 Voltage Low Alarm threshold      = 2.850V
SFP+ 1 Bias Low Alarm threshold         = 2.600mA
SFP+ 1 TX Power Low Alarm threshold     = 0.158mW
SFP+ 1 RX Power Low Alarm threshold     = 0.040mW
==================================
SFP+ 1 Temp High Warning threshold      = 75.000C
SFP+ 1 Voltage High Warning threshold   = 3.630V
SFP+ 1 Bias High Warning threshold      = 8.500mA
SFP+ 1 TX Power High Warning threshold  = 0.741mW
SFP+ 1 RX Power High Warning threshold  = 1.259mW
SFP+ 1 Temp Low Warning threshold       = -5.000C
SFP+ 1 Voltage Low Warning threshold    = 2.970V
SFP+ 1 Bias Low Warning threshold       = 3.000mA
SFP+ 1 TX Power Low Warning threshold   = 0.178mW
SFP+ 1 RX Power Low Warning threshold   = 0.063mW
==================================
SFP+ 1 Temperature                      = 34.988C
SFP+ 1 Voltage                          = 3.281V
SFP+ 1 Tx Bias Current                  = 6.746mA
SFP+ 1 Tx Power                         = 0.635mW
SFP+ 1 Rx Power                         = 0.002mW
==================================
```

```
SFP+ 1 Data Ready state Bar             = False
SFP+ 1 Rx LOS state                     = True
SFP+ 1 Tx Fault state                   = False
SFP+ 1 Rate Select state                = True
SFP+ 1 RS state                         = False
SFP+ 1 Tx Disable state                 = False
=================================
SFP+ 1 Temperature High Alarm Flag      = False
SFP+ 1 Voltage High Alarm Flag          = False
SFP+ 1 Tx Bias High Alarm Flag          = False
SFP+ 1 Tx Power High Alarm Flag         = False
SFP+ 1 Rx Power High Alarm Flag         = False
SFP+ 1 Temperature Low Alarm Flag       = False
SFP+ 1 Voltage Low Alarm Flag           = False
SFP+ 1 Tx Bias Low Alarm Flag           = False
SFP+ 1 Tx Power Low Alarm Flag          = False
SFP+ 1 Rx Power Low Alarm Flag          = True
=================================
SFP+ 1 Temperature High Warning Flag    = False
SFP+ 1 Voltage High Warning Flag        = False
SFP+ 1 Tx Bias High Warning Flag        = False
SFP+ 1 Tx Power High Warning Flag       = False
SFP+ 1 Rx Power High Warning Flag       = False
SFP+ 1 Temperature Low Warning Flag     = False
SFP+ 1 Voltage Low Warning Flag         = False
SFP+ 1 Tx Bias Low Warning Flag         = False
SFP+ 1 Tx Power Low Warning Flag        = False
SFP+ 1 Rx Power Low Warning Flag        = True
```

Related Commands

- interface — configures a physical interface on the switch.
- show ip interface — displays Layer 3 information about the interface.
- show interfaces — displays information on a specific physical interface or virtual interfaces.
- show inventory — displays the switch type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.

show interfaces vlan

Display VLAN statistics.

C9000 Series

Syntax `show interfaces vlan {vlan-id} [LINE] {description}`

Parameters

vlan-id	Enter the interface VLAN number. The range is from 1 to 4094.
LINE	(OPTIONAL) Enter the name of the VLAN.
description	Displays the VLAN interface information with description.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.7(0.0)	Introduced this command.

Example

```
Dell#show interfaces vlan 10
Vlan 10 is up, line protocol is down
Address is 90:b1:1c:f4:99:ce, Current address is 90:b1:1c:f4:99:ce
Interface index is 1107787786
Internet address is not set
Mode of IPv4 Address Assignment: NONE
DHCP Client-ID: 90b11cf499ce
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 2d17h26m
Queueing strategy: fifo
Time since last interface status change: 2d17h26m
Input Statistics:
     0 packets, 0 bytes
Output Statistics:
     0 packets, 0 bytes, 0 underruns
```

Related Commands show interfaces — displays information on a specific physical interface or virtual interface.

show range

Display all interfaces configured using the `interface range` command.

C9000 Series

Syntax `show range`

Command Modes INTERFACE RANGE (config-if-range)

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4093 VLANs on E-Series ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced.

Example

```
Dell(conf)#interface range peGigE 255/1/2
Dell(conf-if-range-pegi-255/1/2)#show range
interface peGigE255/1/2 - 0
```

Related Commands

- interface — configures a physical interface on the switch.
- show ip interface — displays Layer 3 information about the interfaces.
- show interfaces — displays information on a specific physical interface or virtual interface.

show running-config ecmp-group

Display interfaces, LAG, or LAG link bundles being monitored for uneven traffic distribution using the `ecmp-group monitoring enable` command. The ECMP group could have a LAG or a list of 10G/40 interfaces (not just LAG link-bundles).

C9000 Series

Syntax `show running-config ecmp-group`

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.

Related Commands ecmp-group — configures a mechanism to monitor traffic distribution.

shutdown

Disable an interface.

C9000 Series

Syntax `shutdown`

To activate an interface, use the `no shutdown` command.

Defaults The interface is disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information The `shutdown` command marks a physical interface as unavailable for traffic. To discover if an interface is disabled, use the `show ip interface brief` command. Disabled interfaces are listed as down.

Disabling a VLAN or a port channel causes different behavior. When a VLAN is disabled, the Layer 3 functions within that VLAN are disabled. Layer 2 traffic continues to flow. Entering the `shutdown` command on a port channel disables all traffic on the port channel and the individual interfaces within the port channel. To enable a port channel, enter `no shutdown` on the port channel interface and at least one interface within that port channel.

The `shutdown` and `description` commands are the only commands that you can configure on an interface that is a member of a port channel.

Related Commands interface port-channel — creates a port channel interface.

interface vlan — creates a VLAN.

show ip interface — displays the interface routing status. Add the keyword `brief` to display a table of interfaces and their status.

speed (for 10/100/1000/10000 interfaces)

Set the speed for 10/100/1000/10000 interfaces. Set both sides of a link to the same speed (10/100/1000/10000) or to auto or the link may not come up.

Syntax `speed {10 | 100 | 1000 | 10000 | auto}`

To return to the default setting, use the `no speed {10 | 100 | 1000 | 10000}` command.

Parameters

10	Enter the keyword `10` to set the interface's speed to 10 Mb/s.

NOTE: This interface speed is not supported on the LC-EH-GE-50P or the LC-EJ-GE-50P card. If the command is entered for these interfaces, an error message appears.

100	Enter the keyword `100` to set the interface's speed to 10/100 Mb/s. **NOTE: When this setting is enabled, only 100Base-FX optics are supported on the LC-EH-GE-50P or the LC-EJ-GE-50P card.**
1000	Enter the keyword `1000` to set the interface's speed to 1000 Mb/s. Auto-negotiation is enabled. For more information, refer to `negotiation auto`. **NOTE: When this setting is enabled, only 1000Base-FX optics are supported on the LC-EH-GE-50P or the LC-EJ-GE-50P card.**
10000	Enter the keyword `10000` to set the interface's speed to 10000 Mb/s. Auto-negotiation is enabled. For more information, refer to `negotiation auto`.
auto	Enter the keyword `auto` to set the interface to auto-negotiate its speed. Auto-negotiation is enabled. For more information, refer to `negotiation auto`.

Defaults **auto**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.0)	Added support for fanned–out 1 Gigabit SFP port.
9.9(0.0)	Introduced on the C9010.
9.8(2.0)	Introduced on the S3100 series.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Supported on LC-EH-GE-50P or the LC-EJ-GE-50P cards.
8.1.1.0	Introduced on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information This command is found on the 10/100/1000/10000 Base-T Ethernet interfaces.

When you enable `auto`, the system performs an automatic discovery to determine the optics installed and configure the appropriate speed.

When you configure a speed for the 10/100/1000/10000 interface, confirm the negotiation auto command setting. Both sides of the link must have auto-negotiation either enabled or disabled. For speed settings of 1000 or auto, the software sets the link to auto-negotiation and you cannot change that setting.

NOTE: Starting with Dell Networking OS version 7.8.1.0, when you use a copper SFP2 module with catalog number GP-SFP2-1T in the S25P model of the S-Series, you can manually set its speed with the `speed` command. When you set the speed to 10 or 100 Mbps, you can also use the `duplex` command.

If you use an active optical cable (AOC), you can convert the QSFP+ port to a 10 Gigabit SFP+ port or 1 Gigabit SFP port. You can use the `speed` command to enable the required speed.

speed (Management interface)

Set the speed for the Management interface.

C9000 Series

Syntax

`speed {10 | 100 | auto}`

To return to the default setting, use the `no speed {10 | 100}` command.

Parameters

10	Enter the keyword `10` to set the interface's speed to 10 Mb/s.
100	Enter the keyword `100` to set the interface's speed to 10/100 Mb/s.
auto	Enter the keyword `auto` to set the interface to auto-negotiate its speed.

Defaults

auto

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.11.1	Introduced on the S55, S60, and S4810
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information This command is found on the Management interface only.

Related Commands

- interface ManagementEthernet — configures the Management port on the system (either the Primary or Standby RPM).
- management route — configures a static route that points to the Management interface or a forwarding router.

switchport

Place an interface in Layer 2 mode.

C9000 Series

Syntax `switchport [backup interface {tengigabit` *`slot/port`* `| fortyGigE` *`slot/port`* `| port-channel` *`number`*`}]`

To remove an interface from Layer 2 mode and place it in Layer 3 mode, enter the `no switchport` command. If a switchport backup interface is configured, first remove the backup configuration. To remove a switchport backup interface, enter the `no switchport backup interface {tengigabit slot/port | fortyGigE slot/port | port-channel number}` command.

Parameters

backup interface	Use this option to configure a redundant Layer 2 link without using Spanning Tree. The keywords `backup interface` configures a backup port so that if the primary port fails, the backup port changes to the up state. If the primary later comes up, it becomes the backup.
tengigabit	Enter the keyword `tengigabit` if the backup port is a 10G port.
fortyGigE	Enter the keyword `fortyGigE` if the backup port is a 40G port.
port-channel	Enter the keywords `port-channel` if the backup port is a static or dynamic port channel.
slot/port	Specify the line card and port number of the backup port.

Defaults Disabled (The interface is in Layer 3 mode.)

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.

Version	Description
8.4.1.0	Added support for port-channel interfaces (the `port-channel number` option).
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Added the `backup interface` option.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

If an IP address or VRRP group is assigned to the interface, you cannot use the `switchport` command on the interface. To use the `switchport` command on an interface, only the `no ip address` and `no shutdown statements` must be listed in the `show config` output.

When you enter the `switchport` command, the interface is automatically added to the default VLAN.

To use the `switchport backup interface` command on a port, first enter the `switchport` command. For more information, see the "Configuring Redundant Links" section in the "Layer 2" chapter of the *Dell Networking OS Configuration Guide*.

Related Commands

interface port-channel — creates a port channel interface.

show interfaces switchport — displays information about switchport interfaces.

wavelength

Set the wavelength for tunable 10–Gigabit SFP+ optics.

Syntax

`wavelength`

To retain the existing wavelength, use the `no wavelength` command.

Defaults

none

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.0)	Introduced on the S6000, S6000–ON, S5000, S4810, S4820T, S3048–ON, S4048–ON, M I/O Aggregator, FN I/O Module, MXL, C9010, S3100 series, and Z9100-ON.

Usage Information

The wavelength can be configured only on a tunable 10–Gigabit SFP+ optic. The wavelength range is from 1528.3 nm to 1568.77nm.

If you configure the wavelength on a non-tunable optic, there is no change to the existing wavelength. The configured wavelength is saved in the running configuration and is applicable, when a tunable optic is used.

If you do not configure the wavelength on an inserted tunable optic, the existing wavelength is used.

Example The following example shows the wavelength set for a tunable 10–Gigabit SFP+ optic:

Related Commands

- show config — displays the interface configuration.

Egress Interface Selection (EIS) Commands

The following commands are Egress Interface Selection (EIS) commands.

application

Configure the management egress interface selection.

C9000 Series

Syntax `application {all | application-type}`

To remove a management application configuration, use the `no application {all | application-type}` command.

Parameters

application-type Enter any of the following keywords:

- For DNS, enter the keyword `dns`.
- For FTP, enter the keyword `ftp`.
- For NTP, enter the keyword `ntp`.
- For Radius, enter the keyword `radius`.
- For sFlow collectors, enter the keyword `sflow-collector`.
- For SNMP (traps and MIB responses), enter the keywords `snmp` .
- For SSH, enter the keyword `ssh` .
- For Syslog, enter the keyword `syslog`.
- For TACACS, enter the keyword `tacacs`.
- For Telnet, enter the keyword `telnet`.
- For TFTP, enter the keyword `tftp`.

all Configure all applications.

Defaults None.

Command Modes EIS Mode (conf-mgmt-eis)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

clear management application pkt-cntr

Clear management application packet counters for all management application types.

C9000 Series

Syntax `clear management application pkt-cntr`

Defaults None.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

management egress-interface-selection

To make configured application traffic egress through the management port instead of the front-end (FE) port, enable and configure a management egress interface.

C9000 Series

Syntax `management egress-interface-selection`

To disable and remove management egress interface selection (EIS) configurations, use the `no management egress-interface-selection` command.

Defaults None.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

show ip management-eis-route

Display the management routes used by EIS.

C9000 Series

Syntax `show ip management-eis-route`

Defaults None.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell# show ip management-eis-route
Destination    Gateway                 State      Route Source
-----------    -------                 -----      ------------
10.11.0.0/16   ManagementEthernet 0/0  Connected  Connected
172.16.1.0/24  10.11.192.4             Active     Static
```

show management application pkt-cntr

Display the number of packets for each application type that have taken the management route.

C9000 Series

Syntax `show management application pkt-cntr`

Defaults None.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell# show management application pkt-cntr
dns               :   2
ftp               :   0
ntp               :   0
radius            :   0
sflow-collector   :   0
snmp              :   0
ssh               :   0
syslog            :   0
tacacs            :   0
telnet            :   0
tftp              :   0
```

show management application pkt-fallback-cntr

Display the number of packets for each application type that have been rerouted to the default routing table due to management port or route lookup failure.

C9000 Series

Syntax `show management application pkt—fallback-cntr`

Defaults None.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell# show management application pkt-fallback-cntr
dns               :   0
ftp               :   0
ntp               :   0
radius            :   0
sflow-collector   :   0
```

```
snmp                :    0
ssh                 :    2
syslog              :    0
tacacs              :    0
telnet              :    0
tftp                :    0
```

Port Channel Commands

A Link Aggregation Group (LAG) is a group of links that appear to a MAC client as if they were a single link according to IEEE 802.3ad. In Dell Networking OS, a LAG is also known as a Port Channel.

- The platform supports 4096 port channels and 16 members per port channel.

Because each port can be assigned to only one Port Channel, and each Port Channel must have at least one port, some of those nominally available Port Channels might have no function because they could have no members if there are not enough ports installed.

Port Channel can be configured with port extender (PE) interface when feature extended bridge is enabled.

NOTE: The Dell Networking OS implementation of LAG or Port Channel requires that you configure a LAG on both switches manually. For information about Dell Networking OS link aggregation control protocol (LACP) for dynamic LAGs, see the Link Aggregation Control Protocol (LACP) chapter. For more information about configuring and using Port Channels, see the *Dell Networking OS Configuration Guide*.

channel-member

Add an interface to the Port Channel, while in INTERFACE PORTCHANNEL mode.

C9000 Series

Syntax

`channel-member` *interface*

To delete an interface from a Port Channel, use the `no channel-member interface` command.

Parameters

interface (OPTIONAL) Enter any of the following keywords and slot/port, *peid/stack-unit/port-id*, or number information:

- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults

Not configured.

Command Modes INTERFACE PORTCHANNEL

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information Use the `interface port-channel` command to access this command.

You cannot add an interface to a Port Channel if the interface contains an IP address in its configuration. Only the `shutdown`, `description`, `mtu`, and `ip mtu` commands can be configured on an interface if it is added to a Port Channel. The `mtu` and `ip mtu` commands are only available when the chassis is in Jumbo mode.

Link MTU and IP MTU considerations for Port Channels are:

- All members must have the same link MTU value and the same IP MTU value.
- The Port Channel link MTU and IP MTU must be less than or equal to the link MTU and IP MTU values configured on the channel members. For example, if the members have a link MTU of 2100 and an IP MTU 2000, the Port Channel's MTU values cannot be higher than 2100 for link MTU or 2000 bytes for IP MTU.

When an interface is removed from a Port Channel with the `no channel-member` command, the interface reverts to its configuration prior to joining the Port Channel.

An interface can belong to only one Port Channel.

Related Commands description — assigns a descriptive text string to the interface.

interface port-channel — creates a Port Channel interface.

shutdown — disables/enables the port channel.

group

Group two LAGs in a supergroup (“fate-sharing group” or “failover group”).

C9000 Series

Syntax

`group group_number port-channel number port-channel number`

To remove an existing LAG supergroup, use the `no group group_number` command.

Parameters

group_number	Enter an integer from 1 to 32 that uniquely identifies this LAG fate-sharing group.
port-channel *number*	Enter the keywords `port-channel` then an existing LAG number. Enter this keyword/variable combination twice, identifying the two paired LAGs.

Defaults

none

Command Modes

PORT-CHANNEL FAILOVER-GROUP (conf-po-failover-grp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series, E-Series, and S-Series.

Related Commands

port-channel failover-group — accesses PORT-CHANNEL FAILOVER-GROUP mode to configure a LAG failover group.

show interfaces port-channel — displays information on configured Port Channel groups.

interface port-channel

Create a Port Channel interface, which is a link aggregation group (LAG) containing sixteen physical interfaces on the switch.

C9000 Series

Syntax

`interface port-channel` *`channel-number`*

To delete a Port Channel, use the `no interface port-channel` *`channel-number`* command.

Parameters

channel-number	For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

Defaults

Not configured.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on S4810.
8.3.11.1	Introduced on Z9000.
8.1.1.0	Introduced on E-Series ExaScale.
7.6.1.0	Introduced on S-Series.
7.5.1.0	Introduced on C-Series.
6.2.1.0	Introduced on E-Series.

Usage Information

Port Channel interfaces are logical interfaces and can be either in Layer 2 mode (by using the `switchport` command) or Layer 3 mode (by configuring an IP address) with an exception that when the PE ports are configured as a member of Port Channel you can configure that Port Channel in Layer 2 mode (using the `switchport` command) and add it to a VLAN.

In the Configuration Terminal Batch mode, you can configure the Port Channel in a dual-homing setup.

The `shutdown`, `description`, and `name` commands are the only commands that you can configure on an interface while it is a member of a Port Channel. To add a physical interface to a Port Channel, the interface can

only have the `shutdown`, `description`, and `name` commands configured. The Port Channel's configuration is applied to the interfaces within the Port Channel.

A Port Channel can contain both 100/1000 interfaces and GE interfaces. Based on the first interface configured in the Port Channel and enabled, the system determines if the Port Channel uses 100 Mb/s or 1000 Mb/s as the common speed. For more information, refer to channel-member.

If a port extender (PE) is provisioned, cascade LAGs are created automatically (auto-LAGs). You cannot configure the port-channel created through the auto-LAG. The range for the port-channel created through auto-LAG is from 257 to 513.

If the line card is in a Jumbo mode chassis, you can also configure the `mtu` and `ip mtu` commands. The Link MTU and IP MTU values configured on the channel members must be greater than the Link MTU and IP MTU values configured on the Port Channel interface.

NOTE: In a Jumbo-enabled system, all members of a Port Channel must be configured with the same link MTU values and the same IP MTU values.

Example

```
Dell(conf)# int port-channel 2
Dell(conf-if-po-2)#
```

Related Commands

channel-member — adds a physical interface to the LAG.

interface — configures a physical interface.

interface loopback — configures a Loopback interface.

interface null — configures a null interface.

interface vlan — configures a VLAN.

shutdown — disables/enables the port channel.

minimum-links

Configure the minimum number of links in a LAG (Port Channel) that must be in "oper up" status for the LAG to be also in "oper up" status.

C9000 Series

Syntax `minimum-links number`

Parameters

number	Enter the number of links in a LAG that must be in "oper up" status. The range is from 1 to 16. The default is **1**.

Defaults **1**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

If you use this command to configure the minimum number of links in a LAG that must be in "oper up" status, the LAG must have at least that number of "oper up" links before it can be declared as up. For example, if the required minimum is four, and only three are up, the LAG is considered down.

port-channel failover-group

To configure a LAG failover group, access PORT-CHANNEL FAILOVER-GROUP mode.

C9000 Series

Syntax

```
port-channel failover-group
```

To remove all LAG failover groups, use the `no port-channel failover-group` command.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.

Usage Information

This feature groups two LAGs to work in tandem as a supergroup. For example, if one LAG goes down, the other LAG is taken down automatically, providing an alternate path to reroute traffic, avoiding oversubscription on the other LAG. You can use both static and dynamic (LACP) LAGs to configure failover groups. For more information, refer to the "Port Channel" chapter in the *Dell Networking OS Configuration Guide*.

Related Command

group — groups two LAGs in a supergroup ("fate-sharing group").

show interfaces port-channel — displays information on configured Port Channel groups.

show config

Display the current configuration of the selected LAG.

C9000 Series

Syntax

```
show config
```

Command Modes

INTERFACE PORTCHANNEL

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Example

```
Dell(conf-if-po-1)# show config
!
interface Port-channel 1
  no ip address
  shutdown
Dell(conf-if-po-1)#
```

show interfaces port-channel

Display information on configured Port Channel groups.

C9000 Series

Syntax `show interfaces port-channel [channel-number] [brief]`

Parameters

channel-number	For a Port Channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 128.
brief	(OPTIONAL) Enter the keyword `brief` to display only the port channel number, the state of the port channel, and the number of interfaces in the port channel.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series. Modified to display the LAG failover group status.
7.5.1.0	Introduced on the C-Series.

Usage Information

To view the show output for multiple ports of a specified slot at a time, you can specify any random port number or a range of ports, or a combination of both.

To specify a port range, you can enter a hyphenated range of one or more port range values separated with commas; for example, `show interfaces port—channel 1-2,7`. To enter any random number of ports, you can enter a comma-separated string of port numbers, for example `show interfaces port-channel 1,7`

NOTE: The port-range option is only available for 1 Gigabit Ethernet, 10-Gigabit Ethernet, 40-Gigabit Ethernet, Fast Ethernet, FC, Port Channel, and VLAN interfaces.

The following describes the `show interfaces port-channel` command shown in the following example.

Field	Description
Port-Channel 1...	Displays the LAG's status. In the Example, the status of the LAG's LAG fate-sharing group ("Failover-group") is listed.
Hardware is...	Displays the interface's hardware information and its assigned MAC address.
Port-channel is part...	Indicates whether the LAG is part of a LAG fate-sharing group ("Failover-group").
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
MTU 1554...	Displays link and IP MTU.
LineSpeed	Displays the interface's line speed. For a port channel interface, it is the line speed of the interfaces in the port channel.
Members in this...	Displays the interfaces belonging to this port channel.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the `show interfaces` counters were cleared.
Queueing strategy.	States the packet queuing strategy. FIFO means first in first out.
packets input...	Displays the number of packets and bytes into the interface.
Input 0 IP packets...	Displays the number of packets with IP headers, VLAN tagged headers, and MPLS headers. The number of packets may not add correctly because a VLAN tagged IP packet counts as both a VLAN packet and an IP packet.
0 64-byte...	Displays the size of packets and the number of those packets entering that interface. This information is displayed over two lines.
Received 0...	Displays the type and number of errors or other specific packets received. This information is displayed over three lines.
Output 0...	Displays the type and number of packets sent out the interface. This information is displayed over three lines.
Rate information...	Displays the traffic rate information into and out of the interface. Traffic rate is displayed in bits and packets per second.
Time since...	Displays the time since the last change in the configuration of this interface.

Example (peGigE)

```
Dell(conf)#do sho int po 111
Port-channel 111 is up, line protocol is up
Created by LACP protocol
Hardware address is 34:17:eb:00:21:91, Current address is 34:17:eb:00:21:91
Interface index is 1258348032
Minimum number of links to bring Port-channel up is 1
Internet address is not set
Mode of IPv4 Address Assignment : NONE
DHCP Client-ID :3417eb002191
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 5000 Mbit
Members in this channel:  PeGi 1/0/36(U) PeGi 1/0/37(U) PeGi 1/0/38(U) PeGi
1/0/39(U) PeGi 1/0/46(U)
ARP type: ARPA, ARP Timeout 04:00:00
Queueing strategy: fifo
Input Statistics:
     31035168 packets, 24674745108 bytes
     17 64-byte pkts, 1278919 over 64-byte pkts, 2729921 over 127-byte pkts
     5457788 over 255-byte pkts, 10924046 over 511-byte pkts, 10644476 over
1023-byte pkts
     497 Multicasts, 0 Broadcasts, 31034654 Unicasts
```

```
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     30771019 packets, 24493783827 bytes, 0 underruns
     16 64-byte pkts, 1247561 over 64-byte pkts, 2706754 over 127-byte pkts
     5417155 over 255-byte pkts, 10823333 over 511-byte pkts, 10576198 over
1023-byte pkts
     481 Multicasts, 0 Broadcasts, 30770539 Unicasts
     0 throttles, 0 discarded, 0 collisions, 0 wreddrops
Rate info (interval 299 seconds):
     Input 1555.00 Mbits/sec,     244550 packets/sec, 31.88% of line-rate
     Output 676.00 Mbits/sec,     106216 packets/sec, 13.86% of line-rate
Time since last interface status change: 00:01:41
```

Example

```
Dell# show interfaces port-channel 20
Port-channel 20 is up, line protocol is up (Failover-group 1 is down)
Hardware address is 00:01:e8:01:46:fa
Port-channel is part of failover-group 1
Internet address is 1.1.120.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 2000 Mbit
Members in this channel: Te 0/5 Te 0/18
ARP type: ARPA, ARP timeout 04:00:00
Last clearing of "show interfaces" counters 00:00:00
Queueing strategy: fifo
  44507301 packets input, 3563070343 bytes
  Input 44506754 IP Packets, 0 Vlans 0 MPLS
  41 64-byte pkts, 44502871 over 64-byte pkts, 249 over 127-byte pkts
  407 over 255-byte pkts, 3127 over 511-byte pkts, 606 over 1023-byte pkts
  Received 0 input symbol errors, 0 runts, 0 giants, 0 throttles
  0 CRC, 0 IP Checksum, 0 overrun, 0 discarded
  1218120 packets output, 100745130 bytes, 0 underruns
  Output 5428 Multicasts, 4 Broadcasts, 1212688 Unicasts
  1216142 IP Packets, 0 Vlans, 0 MPLS
  0 throttles, 0 discarded
Rate info (interval 299 sec):
  Input 01.50Mbits/sec, 2433 packets/sec
  Output 00.02Mbits/sec,4 packets/sec
Time since last interface status change: 00:22:34

Dell#
```

Usage Information

The following describes the `show interfaces port-channel brief` command shown in the following example.

Field	Description
LAG	Lists the port channel number.
Mode	Lists the mode: • L3 — for Layer 3 • L2 — for Layer 2
Status	Displays the status of the port channel. • down — if the port channel is disabled (`shutdown`) • up — if the port channel is enabled (`no shutdown`)
Uptime	Displays the age of the port channel in hours:minutes:seconds.
Ports	Lists the interfaces assigned to this port channel.
(untitled)	Displays the status of the physical interfaces (up or down).

Field	Description
	• In Layer 2 port channels, an * (asterisk) indicates which interface is the primary port of the port channel. The primary port sends out interface PDU. • In Layer 3 port channels, the primary port is not indicated.

Example

```
Dell# sh int por 1 br

LAG Mode Status Uptime    Ports
1   L2   up     00:00:08  Te 2/0  (Up) *
                          Te 2/1 (Down)
                          Te 2/2 (Up)
Dell#
```

Example (port-range)

```
Dell#show interfaces port-channel 1-2 brief
Codes: L - LACP Port-channel
       O - OpenFlow Controller Port-channel
       A - Auto Port-channel
       I - Internally Lagged

    LAG  Mode  Status       Uptime      Ports
    1    L3    down         00:00:00    Te 11/1    (Down)
```

Related Commands

show lacp — displays the LACP matrix.

show port-channel-flow

Display an egress port in a given port-channel flow.

C9000 Series

Syntax

```
show port-channel-flow outgoing-port-channel number incoming-interface
interface {source-ip address destination-ip address} | {source-port number
destination-port number} | {src-mac address dest-mac address {vlan vlanid |
ether-type}}
```

Parameters

outgoing-port-channel *number*

Enter the keywords `outgoing-port-channel` then the number of the port channel to display flow information.

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

incoming-interface *interface*

Enter the keywords `incoming-interface` then the interface type and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Gigabit Ethernet interface, enter the keyword `gigabitethernet` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *peid/stack-unit/port-pipe id* information.

- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

NOTE: The peGigE or peTenGigE option is available only when the extended bridge feature is enabled.

source-ip *address*	Enter the keywords `source-ip` then the IP source address in IP address format.
destination-ip *address*	Enter the keywords `destination-ip` then the IP destination address in IP address format.
source-port *number*	Enter the keywords `source-port` then the source port number. The range is from 1 to 65536. The default is **None**.
destination-port *number*	Enter the keywords `destination-port` then the destination port number. The range is from 1 to 65536. The default is **None**.
source-mac *address*	Enter the keywords `source-mac` then the MAC source address in the nn:nn:nn:nn:nn:nn format.
destination-mac *address*	Enter the keywords `destination-mac` then the MAC destination address in the nn:nn:nn:nn:nn:nn format.
vlan ***vlan-id***	Enter the keywords `vlan` then the VLAN-id. The range is from 0 to 4094.
ether-type	Enter the keywords `ether-type` in the XX:XX format.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.

Usage Information Because this command calculates based on a Layer 2 hash algorithm, use this command to display flows for switched Layer 2 packets, not for routed packets (use the `show ip flow` command to display routed packets).

The `show port-channel-flow` command returns the egress port identification in a given port-channel if a valid flow is entered. A mismatched flow error occurs if MAC-based hashing is configured for a Layer 2 interface and you are trying to display a Layer 3 flow.

The output displays three entries:

- Egress port for unfragmented packets.
- In the event of fragmented packets, the egress port of the first fragment.

- In the event of fragmented packets, the egress port of the subsequent fragments.

NOTE: In the `show port channel flow` command output, the egress port for an unknown unicast, multicast, or broadcast traffic is not displayed.

The following example shows the `show port-channel-flow outgoing-port-channel` *number* `incoming-interface` *interface* `source-mac` *address* `destination-mac` *address*

- Load-balance is configured for MAC
- Load-balance is configured for IP 4-tuple/2-tuple
- A non-IP payload is going out of Layer 2 LAG interface that is a member of VLAN with an IP address

Example

```
Dell#show port-channel-flow port-channel 1 incoming-interface te 2/0
source-mac 00:00:50:00:00:00 destination-mac 00:00:a0:00:00:00

    Egress Port for port-channel 1, for the given flow, is Te 2/1
```

Example: peGigE

```
Dell#show port-channel-flow port-channel 111 incoming-interface pegigE
111/0/33
src-mac 00:01:0b:00:00:00  dest-mac 00:01:0b:00:03:00 vlan 111 ether-type ff:ff

Egress Port information for port-channel 111, for the given flow,is
PeGi 111/0/38.
```

HiGig Port Channel Commands

High-Gigabit Ethernet (HiGig) port channels are used to transmit data between internal backplane ports on line-card (leaf) and switch fabric module (SFM - spine) network processing units (NPUs). You can configure an SNMP trap to be generated when traffic distribution in a HiGig port channel is uneven.

NOTE: HiGig port channels on the backplane are also referred to as *HiGig link bundles* .

The backplane port channels operate as HiGig link bundles to transmit data traffic between line-card and SFM NPUs. There are 10 line-cards and 2 SFM NPUs. The 6 SFM (spine) NPUs comprise the switch fabric module.

Each line-card has one NPU numbered 0. SFM NPUs are numbered 0 to 1.

Line-card and SFM NPUs use HiGig port channels to transmit data.

- An SFM NPU uses 10 HiGig port channels, one port channel to transmit data to each line-card NPU. Each HiGig port channel in an SFM NPU consists of three HiGig links.
- A line-card NPU supports 24 front-end I/O ports and six backplane HiGig ports. The six backplane links are members of two HiGig port channel that connects the line-card NPU to each SFM NPU. Three HiGig links in the port channel are used to connect to each SFM NPU.

clear hardware hg-stats

Clear traffic statistics from a HiGig port in a HiGig link bundle/port channel on a line-card or switch fabric module (SFM) NPU.

C9000 Series

Syntax

```
clear hardware {sfm npu-id | linecard slot} hg-stats {port hg-port—number |
unit npu-id port hg-port—number}
```

Parameters

sfm *npu-id*	Specify a switch SFM (spine) NPU by entering the keyword `sfm` and SFM NPU ID. Valid SFM NPU IDs are 0 to 1.
linecard *slot*	Specify a line-card (leaf) NPU by entering the keyword `linecard` and line-card slot. Valid slot numbers are 0 to 11.
hg-stats {port *hg-port-number* | unit *npu-id* port *hg-port-number*}	Enter the keyword `hg-stats` to clear HiGig port statistics. For an SFM NPU HiGig link bundle, specify only a HiGig port number. Valid SFM *hg-port-number* values are 1 to 33. For a line-card NPU HiGig link bundle, specify an NPU ID and a HiGig port number. Line-card NPU value is 0. Line-card HiGig port numbers range from 27 to 32.

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.1.0	Introduced on the Z9500 .
9.3.0.0	Added support for the `hg-stats` option on the Z9000 platform.

Example

```
Dell#clear hardware linecard 0 hg-stats unit 0 port 27


Dell#show hardware linecard 0 hg-stats unit 0 port 27
Higig Port Statistics:
HiGigabitEthernet 0/0/27,
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes 0 underruns
     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 Multicasts, 0 Broadcasts 0 Unicasts
     0 throttles, 0 discarded, 0 collisions 0 wredDrops
     0 Green WredDrops 0 Yellow WredDrops, 0 Red WredDrops
Rate info (interval 15 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
```

Related Commands show hardware hg-stats — displays traffic statistics from internal ports in a HiGig link bundle.

hg-link-bundle-monitor enable

Enable the monitoring of link utilization and traffic distribution in backplane HiGig link bundles/port channels on a line-card or switch fabric module (SFM) NPU.

C9000 Series

Syntax

`hg-link-bundle-monitor {sfm` *`npu-id`* `hg-port—channel` *`hg-port—channel-id`* `| slot` *`slot`* `npuUnit` *`npu-id`* `hg-port—channel 0} enable`

To disable HiGig link-bundle monitoring, use the `no` version of this command.

Parameters

sfm *npu-id* hg-port-channel *hg-port-channel-id*	Specify a HiGig port channel on a switch SFM (spine) NPU by entering the keyword `sfm` and SFM NPU ID, then `hg-port-channel` and a HiGig port channel ID. SFM NPU IDs are 0 to 1; SFM HiGig port-channel IDs are 0 to 10.
slot *slot-id* npuUnit *npu-id* hg-port-channel 0	Specify a HiGig port channel on a line-card (leaf) NPU by entering the keyword `slot` and slot number, then `npuUnit` and line-card NPU ID, then `hg-port-channel 0`. Line-card slot numbers are 0 to 11; line-card NPU ID is 0 . The HiGig port-channel ID range is from 0 to 2.
enable	Enable HiGig link-bundle monitoring.

Command Mode

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.3.0.0	Introduced on the Z9000 switch.

Usage Information

You can configure HiGig link bundle monitoring so that a system log message or an SNMP trap is generated when traffic distribution in a bundle is uneven. The formula that determines uneven traffic distribution is predefined.

hg-link-bundle-monitor rate-interval

Specify the interval (in seconds) for polling traffic distribution in the member links of a HiGig link bundle.

C9000 Series

Syntax

`hg-link-bundle-monitor rate-interval` *`seconds`*

To restore the default value, use the `no` version of this command.

Parameters

seconds	Polling interval in seconds. The valid values are from 10 to 299.

Command Mode

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500 switch.
9.3.0.0	Introduced on the Z9000 switch.

Defaults The default polling interval for HiGig link bundles is 15 seconds.

Usage Information The rate interval used to poll member links is globally configured and applied to all HiGig link bundles in the system.

hg-link-bundle-monitor trigger-threshold

Specify the bandwidth-percentage threshold used in HiGig link-bundle monitoring to determine uneven traffic distribution and when an alarm is generated.

C9000 Series

Syntax `hg-link-bundle-monitor trigger-threshold` *percentage*

To restore the default value, use the `no` version of this command.

Parameters

percentage	Trigger threshold (in percentage of link-bundle bandwidth) at which an SNMP trap is generated. Valid values are 1 to 90.

Command Modes CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.1.0	Introduced on the Z9500.
9.3.0.0	Introduced on the Z9000 platform.

Defaults The default trigger-threshold value is 60.

Usage Information The trigger-threshold of bandwidth usage, which determines when the calculation of link-bundle utilization is performed, is set at 60 percent of the link-bundle bandwidth. When the total traffic use (mean) is below the trigger-threshold percentage, unevenness in link-bundle traffic distribution is not reported. If traffic unevenness is detected in three consecutive measurements, an alarm is issued. The time interval between measurements is defined by the rate interval for HiGig link polling (default 15 seconds).

show hardware hg-stats

Display the traffic statistics from internal ports in a HiGig link bundle/port channel on a line-card or switch fabric module (SFM) NPU.

C9000 Series

Syntax

```
show hardware {sfm npu-id | linecard slot} hg-stats {port hg-port—number | unit npu-id port hg-port—number}
```

Parameters

sfm *npu-id*	Specify a switch SFM (spine) NPU by entering the keyword `sfm` and SFM NPU ID. Valid SFM NPU IDs are 0 to 1.
linecard *slot*	Specify a line-card (leaf) NPU by entering the keyword `linecard` and line-card slot. Valid slot numbers are 0 to 11.
hg-stats {port *hg-port-number* | unit *npu-id* port *hg-port-number*}	Enter the keyword `hg-stats` to display HiGig port statistics. For an SFM NPU HiGig link bundle, specify only a HiGig port number. Valid SFM *hg-port-number* values are 1 to 33. For a line-card NPU HiGig link bundle, specify an NPU ID and a HiGig port number. Line-card NPUs range is 0. Line-card HiGig port numbers range from 27 to 32.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.3.0.0	Added support for the `hg-stats` option on the Z9000 platform.
9.2.1.0	Introduced on the Z9500.

Example (Line-card HiGig Port)

```
Dell#show hardware linecard 0 hg-stats unit 0 port 27
Higig Port Statistics:
HiGigabitEthernet 0/0/27,
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes 0 underruns
     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 Multicasts, 0 Broadcasts 0 Unicasts
     0 throttles, 0 discarded, 0 collisions 0 wredDrops
     0 Green WredDrops 0 Yellow WredDrops, 0 Red WredDrops
Rate info (interval 15 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
```

```
Dell#
Dell#show hardware sfm 0 hg-stats port 1
Higig Port Statistics:
HiGigabitEthernet 10/0/1,
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     0 packets, 0 bytes 0 underruns
     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 Multicasts, 0 Broadcasts 0 Unicasts
     0 throttles, 0 discarded, 0 collisions 0 wredDrops
     0 Green WredDrops 0 Yellow WredDrops, 0 Red WredDrops
Rate info (interval 15 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
```

Example (SFM HiGig Port)

```
Dell# show hardware sfm 5 hg-stats port 19
Higig Port Statistics:
HiGigabitEthernet 3/5/19,
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     63970532045 packets, 5117642582960 bytes 0 underruns
     0 64-byte pkts, 63970531981 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 Multicasts, 0 Broadcasts 63970532058 Unicasts
     0 throttles, 0 discarded, 0 collisions 0 wredDrops
Rate info (interval 15 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 37096.40 Mbits/sec,   57963128 packets/sec, 94.88% of line-rate
```

Example (SFM HiGig Port)

```
Dell# show hardware sfm 5 hg-stats port 19
Higig Port Statistics:
HiGigabitEthernet 3/5/19,
Input Statistics:
     0 packets, 0 bytes
     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 Multicasts, 0 Broadcasts
     0 runts, 0 giants, 0 throttles
     0 CRC, 0 overrun, 0 discarded
Output Statistics:
     63970532045 packets, 5117642582960 bytes 0 underruns
     0 64-byte pkts, 63970531981 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 Multicasts, 0 Broadcasts 63970532058 Unicasts
     0 throttles, 0 discarded, 0 collisions 0 wredDrops
Rate info (interval 15 seconds):
     Input 00.00 Mbits/sec,          0 packets/sec, 0.00% of line-rate
     Output 37096.40 Mbits/sec,   57963128 packets/sec, 94.88% of line-rate
```

Related Commands clear hardware hg-stats — clears traffic statistics from internal ports in a HiGig link bundle.

show hg-link-bundle-distribution

Display the operational status and link utilization in a HiGig link bundle.

C9000 Series

Syntax

```
show hg-link-bundle-distribution {sfm npu-id hg-port—channel hg-port—channel-id
| slot slot npuUnit npu-id hg-port—channel 0} enable
```

Parameters

sfm *npu-id* hg-port-channel *hg-port-channel-id*	Specify a HiGig port channel on a switch SFM (spine) NPU by entering the keyword `sfm` and SFM NPU ID, then `hg-port-channel` and a HiGig port channel ID. SFM NPU ID is 0; SFM HiGig port-channel IDs are 0 to 10.
slot *slot-id* npuUnit *npu-id* hg-port-channel 0	Specify a HiGig port channel on a line-card (leaf) NPU by entering the keyword `slot` and slot number, then `npuUnit` and NPU ID, then `hg-port-channel 0`. Line-card slot numbers are 0 to 11; line-card NPU ID is 0. The HiGig port-channel ID is from 0 to 2.

Command Modes

EXEC, EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.(1.0)	Introduced on the Z9500.
9.3.0.0	Introduced on the Z9000.

Usage Information

The following table illustrates the fields displayed in the output of this command:

Table 4. `show hg-link-bundle-distribution` Command Description

Field	Description
Link-bundle trigger threshold	Percentage value of link-bundle bandwidth that serves as the threshold for marking a link bundle as being overutilized, triggering link-bundle monitoring, and generating an SNMP alarm.
Slot	Slot number of a line card.
npuUnit	Network processing unit (NPU) ID number of a HiGig link bundle/port-channel.
hg-port-channel	Port-channel number of a HiGig link bundle.
Utilization (In Percent)	Percentage of total bandwidth usage by the traffic transmitted on the HiGig link bundle.
Alarm State	Indicates whether an alarm has been generated if uneven traffic distribution occurs in a HiGig link bundle. Possible values are Active and Inactive.
Interface	Member interface of the specified HiGig link bundle/ port channel in the format:

Field	Description
	slot-id/npu-id:hg*higig-port-number*
Utilization (In Percent)	Percentage of total link-bundle bandwidth used on each member link.

Example

```
Dell#show hg-link-bundle-distribution slot 0 npu 0 hg-port-channel 0

hg-link-bundle trigger threshold - 60

HiGigabitEthernet Link Bundle 0/0/0,
  Utilization [In Percent] - 0 Alarm State - Inactive

Interface Utilization [In Percent]

0/0:hg27          0

0/0:hg28          0

0/0:hg29          0
```

snmp-server enable traps hg-lbm

Enable the generation of SNMP traps and notifications when HiGig link-bundle monitoring is enabled.

C9000 Series

Syntax `snmp-server enable traps hg-lbm`

Parameters

hg-lbm	Enter the keyword `hg-lbm` to enable traps for HiGig link-bundle monitoring.

Command Modes CONFIGURATION mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.1.0	Introduced on the Z9500.
9.3.0.0	Introduced on the Z9000.

Time Domain Reflectometer (TDR) Commands

TDR is useful for troubleshooting an interface that is not establishing a link; either it is flapping or not coming up at all. TDR detects open or short conditions of copper cables on 100/1000 Base-T modules.

Important Points to Remember

- The interface and port must be enabled (configured—refer to the `interface` command) before running TDR. An error message is generated if you have not enabled the interface.

- The interface on the far-end device must be shut down before running TDR.
- Because TDR is an intrusive test on an interface that is not establishing a link, do not run TDR on an interface that is passing traffic.
- When testing between two devices, do not run the test on both ends of the cable.

tdr-cable-test

Test the condition of copper cables on 100/1000 Base-T modules.

Syntax `tdr-cable-test interface`

Parameters

interface	Enter the keyword `TenGigabitEthernet` , `peGigE` or `peTenGigE` then the slot/port information for the 100/1000 Ethernet interface.

Defaults None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.10(0.1)	Introduced on the S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.9(0.0)	Introduced on the C9010.
9.8(2.0)	Introduced on the S3100 series.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7.0.0	Introduced on the S5000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series.
7.7.1.0	Introduced on the S Series.
7.6.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The interface must be enabled to run the test or an error message is generated:

```
DellEMC# tdr-cable-test tengigabitethernet 11/1
% Error: Interface is disabled Te 11/1.
```

Syslog messages are generated when the link flaps during TDR tests.

In a dual homing setup, you can use this command only from the primary VLT peer.

Related Commands

- show tdr — display the results of the TDR test.

show tdr

Display the TDR test results.

Syntax

```
show tdr interface
```

Parameters

interface	Enter the keyword `TenGigabitEthernet` , `peGigE` or `peTenGigE` then the slot/port information for the 100/1000 Ethernet interface.

Defaults

None

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.10(0.1)	Introduced on the S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.9(0.0)	Introduced on the C9010.
9.8(2.0)	Introduced on the S3100 series.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7.0.0	Introduced on the S5000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.1.1.0	Introduced.

Usage Information

If the TDR test has not been run, an error message is generated:

```
%Error: Please run the TDR test first
```

The following describes the TDR test status.

Status	Definition
OK Status: Terminated	TDR test is complete, no fault is detected on the cable, and the test is terminated.

Status	Definition
Length: 92 (+/- 1) meters, Status: Shorted	A short is detected on the cable. The location, in this Example is 92 meters. The short is accurate to plus or minus one meter.
Length: 93 (+/- 1) meters, Status: Open	An opening is detected on the cable. The location, in this Example is 93 meters. The open is accurate to plus or minus one meter.
Status: Impedance Mismatch	There is an impedance mismatch in the cables.

Example

```
DellEMC# show tdr tengigabitethernet 11/2
Time since last test: 00:00:11
  Pair A, Length: OK Status: Terminated
  Pair B, Length: OK Status: Terminated
  Pair C, Length: OK Status: Terminated
  Pair D, Length: OK Status: Terminated
```

Related Commands

- tdr-cable-test — run the TDR test.

23

Intermediate System to Intermediate System (IS-IS)

The intermediate system to intermediate system (IS-IS) is an interior gateway protocol that uses a shortest-path-first algorithm. IS-IS facilitates the communication between open systems, supporting routers passing both IP and OSI traffic.

A router is considered an intermediate system. Networks are partitioned into manageable routing domains, called areas. Intermediate systems send, receive, and forward packets to other routers within their area (Level 1 and Level 1-2 devices). Only Level 1-2 and Level 2 devices communicate with other areas.

IS-IS protocol standards are listed in the Standard Compliance chapter in the *Dell Networking OS Configuration Guide*.

NOTE: The fundamental mechanisms of IS-IS are the same between IPv4 and IPv6. Where there are differences between the two versions, they are identified and clarified in this chapter. Except where identified, the information in this chapter applies to both protocol versions.

Topics:

- adjacency-check
- advertise
- area-password
- clear isis
- clns host
- debug isis
- debug isis adj-packets
- debug isis graceful-restart
- debug isis local-updates
- debug isis snp-packets
- debug isis spf-triggers
- debug isis update-packets
- default-information originate
- description
- distance
- distribute-list in
- distribute-list out
- distribute-list redistributed-override
- domain-password
- graceful-restart ietf
- graceful-restart interval
- graceful-restart restart-wait
- graceful-restart t1
- graceful-restart t2
- graceful-restart t3
- hello padding
- hostname dynamic

- ignore-lsp-errors
- ip router isis
- ipv6 router isis
- isis circuit-type
- isis csnp-interval
- isis hello-interval
- isis hello-multiplier
- isis hello padding
- isis ipv6 metric
- isis metric
- isis network point-to-point
- isis password
- isis priority
- is-type
- log-adjacency-changes
- lsp-gen-interval
- lsp-mtu
- lsp-refresh-interval
- max-area-addresses
- max-lsp-lifetime
- maximum-paths
- metric-style
- multi-topology
- net
- passive-interface
- redistribute
- redistribute bgp
- redistribute ospf
- router isis
- set-overload-bit
- show config
- show isis database
- show isis graceful-restart detail
- show isis hostname
- show isis interface
- show isis neighbors
- show isis protocol
- show isis traffic
- spf-interval

adjacency-check

Verify that the “protocols supported” field of the IS-IS neighbor contains matching values to this router.

C9000 Series

Syntax

```
adjacency-check
```

To disable adjacency check, use the `no adjacency-check` command.

Defaults

Enabled.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Introduced on the E-Series.

Usage Information

To perform protocol-support consistency checks on hello packets, use this command. The adjacency-check is enabled by default.

If a BFD session goes down indicating that IPv4 or IPv6 connectivity to its neighbor is lost, it does not imply that the adjacency is lost altogether. The hello adjacency runs over Layer 2, and does not require IP connectivity. However, if IPv4 connectivity is lost to a neighbor, then when the next SPF calculation is performed, the system ensures that it does not calculate any IPv4 or IPv6 routes through that neighbor.

advertise

Leak routes between levels (distribute IP prefixes between Level 1 and Level 2 and vice versa).

C9000 Series

Syntax

`advertise {level1-into-level2 | level2-into-level1} prefix-list-name`

To return to the default, use the `no advertise {level1-into-level2 | level2-into-level1} [prefix-list-name]` command.

Parameters

level1-into-level2	Enter the keywords `level1-into-level2` to advertise Level 1 routes into Level 2 LSPs. This setting is the default.
level2-into-level1	Enter the keywords `level2-into-level1` to advertise Level 2 inter-area routes into Level 1 LSPs. This behavior is described in RFC 2966.
prefix-list-name	Enter the name of a configured IP prefix list. Routes meeting the criteria of the IP Prefix list are leaked.

Defaults

level1-into-level2 (Level 1 to Level 2 leaking enabled and Level 2 to Level 1 leaking is disabled.)

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Added IPv6 ISIS support.
6.3.1.0	Version 6.3.1.0 Introduced

Usage Information

You cannot disable leaking from one level to another; however, you can regulate the rate flow from one level to another using an IP Prefix list. If you do not configure the IP Prefix list, all routes are leaked.

You cannot enable leaking from Level 2 to Level 1, conditional route leaking can be enabled via IP prefix-list.

You can find more information in IETF RFC 2966, *Domain-wide Prefix Distribution with Two-Level IS-IS*.

area-password

Configure a hash message authentication code (HMAC) password for an area.

C9000 Series

Syntax

```
area-password [hmac-md5 | encryption-type] password
```

To delete a password, use the `no area-password` command.

Parameters

hmac-md5	(OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password.
encryption-type	(OPTIONAL) Enter `7` to encrypt the password using DES.
password	Enter a 1 to 16-character length alphanumeric string to prevent unauthorized access or incorrect routing information corrupting the link state database. The password is processed as plain text, which only provides limited security.

Defaults

Not configured.

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

To prevent the link state database from receiving incorrect routing information from unauthorized routers, use the `area-password` command on routers within an area.

The configured password injects into Level 1 LSPs, CSNPs, and PSNPs.

Related Commands

- domain-password — allows you to set the authentication password for a routing domain.
- isis password — allows you to configure an authentication password for an interface.

clear isis

Restart the IS-IS process. All IS-IS data is cleared.

C9000 Series

Syntax `clear isis [vrf vrf-name] [tag] {* | database | traffic}`

Parameters

vrf *vrf-name*	(Optional) Enter the keyword `vrf` followed by the name of the VRF to restart the IS-IS process corresponding to that VRF.
tag	(Optional) Enter an alphanumeric string to specify the IS-IS routing tag area.
*****	Enter the keyword `*` to clear all IS-IS information and restart the IS-IS process. This command removes IS-IS neighbor information and IS-IS LSP database information and the full SPF calculation is done.
database	Clears IS-IS LSP database information.
traffic	Clears IS-IS counters.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000–ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

clns host

Define a name-to-network service mapping point (NSAP) that you use with commands that require NSAPs and system IDs.

C9000 Series

Syntax `clns host name nsap`

Parameters

name	Enter an alphanumeric string to identify the name-to-NSAP mapping.
nsap	Enter a specific NSAP address that is associated with the name parameter.

Defaults Not configured.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information To configure a shortcut name that you can use instead of entering a long string of numbers associated with an NSAP address, use this command.

Related Commands hostname dynamic — enables dynamic learning of host names from routers in the domain and allows the routers to advertise the host names in LSPs.

debug isis

Enable debugging for all IS-IS operations.

C9000 Series

Syntax `debug isis`

To disable debugging of IS-IS, use the `no debug isis` command.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

Entering `debug isis` enables all debugging parameters.

To display all debugging information in one output, use this command. To turn off debugging, you normally enter separate `no` forms of each command. To disable all debug messages for IS-IS at once, enter the `no debug isis` command.

debug isis adj-packets

Enable debugging on adjacency-related activity such as hello packets that are sent and received on IS-IS adjacencies.

C9000 Series

Syntax

`debug isis adj-packets [interface][vrf vrf-name]`

To turn off debugging, use the `no debug isis adj-packets [interface][vrf vrf-name]` command.

Parameters

vrf *vrf-name*	(Optional) Enter the keyword vrf followed by the name of the VRF to enable the debug information on IS-IS for an adjacency tied to that VRF. This command displays the IIH related debug details.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.

Version	Description
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

debug isis graceful-restart

Enable debugging information on IS-IS GR hello, internal state, and event debugs.

C9000 Series

Syntax

`debug isis graceful-retart [vrf vrf-name] [all | events | hello | states]`

To turn off debugging, use the `no debug isis [vrf vrf-name] spf-triggers` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to enable debugging information on IS-IS corresponding to that VRF. This information contains graceful-restart details tied to the VRF that you specify. This information includes GR Hello, Internal State, and Event Debug details.
all	Enter the keyword `all` to enable debugging information that includes all the logs that are related to graceful-restart.
events	Enter the keyword `events` to enable debugging information that includes logs that are related to generated events.
hello	Enter the keyword `hello` to enable debugging information that includes restart TLV related information.
states	Enter the keyword `states` to enable debugging information that includes state machine related information.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms,refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.

debug isis local-updates

To debug IS-IS local update packets, enable debugging on a specific interface and provides diagnostic information.

C9000 Series

Syntax

`debug isis local-updates [interface][vrf vrf-name]`

To turn off debugging, use the `no debug isis [vrf vrf–name] updates [interface]` command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to enable the debugging information on IS-IS corresponding to that VRF. This information contains local updates tied to the VRF that you specify. This command displays the local LSP debugging details of the current unit.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
6.3.1.0	Introduced.

debug isis snp-packets

To debug IS-IS complete sequence number PDU (CSNP) and partial sequence number PDU (PSNP) packets, enable debugging on a specific interface and provides diagnostic information.

C9000 Series

Syntax

`debug isis snp-packets [interface][vrf vrf-name]`

To turn off debugging, use the `no debug isis [vrf vrf-name] snp-packets [interface]` command.

Parameters

interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
vrf *vrf-name*	(Optional) Enter the keyword `vrf` followed by the name of the VRF to enable debugging information on ISIS for CSNP/PSNP packets tied to that VRF. The command displays the SNP (CSNP/PSNP) related debugging information.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
6.3.1.0	Introduced.

debug isis spf-triggers

Enable debugging on the events that triggered IS-IS shortest path first (SPF) events for debugging purposes.

C9000 Series

Syntax

`debug isis [vrf vrf-name] spf-triggers`

To turn off debugging, use the `no debug isis [vrf vrf-name] spf-triggers` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword vrf followed by the name of the VRF to enable debugging information on IS-IS corresponding to that VRF. This information contains spf trigger detail tied to the VRF that you specify. When SPF is triggered, this debugging information is displayed.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms,refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
6.3.1.0	Introduced.

debug isis update-packets

Enable debugging on link state PDUs (LSPs) that a router detects.

C9000 Series

Syntax

`debug isis update-packets [interface][vrf vrf-name]`

To turn off debugging, use the `no debug isis update-packets [interface]` command.

Parameters

interface (OPTIONAL) Identifies the interface type slot/port as one of the following:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port/subport information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

vrf *vrf-name* (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to enable the debugging information on IS-IS. This information contains updates from neighbors tied to the VRF that you specify. This command displays the debugging details of the received LSPs from the neighbors.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
6.3.1.0	Introduced.

default-information originate

Generates a default route into an IS-IS routing domain and controls the distribution of default information.

C9000 Series

Syntax `default-information originate [always] [metric` *`metric`*`] [route-map` *`map-name`*`]`

To disable the generation of a default route into the specified IS-IS routing domain, use the `no default-information originate [always] [metric` *`metric`*`] [route-map` *`map-name`*`]` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to have the default route always advertised.
metric *metric*	(OPTIONAL) Enter the keyword `metric` then a number to assign to the route. The range is from 0 to 16777215.
route-map *map-name*	(OPTIONAL) A default route the routing process generates if the route map is satisfied.

Defaults

Not configured.

Command Modes

- ROUTER ISIS (for IPv4)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (for IPv6)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Added IPv6 ISIS support.
6.3.1.0	Introduced.

Usage Information

When you use this command to redistribute routes into a routing domain, the router becomes an autonomous system (AS) boundary router. An AS boundary router does not always generate a default route into a routing domain. The router still requires its own default route before it can generate one.

How a metric value assigned to a default route advertises depends on the `metric-style` command configuration. If the `metric-style` command is set for Narrow mode and the metric value in the `default-information originate` command is set to a number higher than 63, the metric value advertised in the LSPs is 63. If the `metric-style` command is set for Wide mode, the metric value in the `default-information originate` command is advertised.

Related Commands

- redistribute — redistributes routes from one routing domain to another routing domain.

description

Enter a description of the IS-IS routing protocol.

C9000 Series

Syntax `description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the IS-IS protocol (80 characters maximum).

Defaults none

Command Modes ROUTER ISIS

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
pre-7.7.1.0	Introduced.

Related Commands router isis — Enter ROUTER mode on the switch.

distance

Define the administrative distance for learned routes.

C9000 Series

Syntax `distance weight [ip-address mask [prefix-list]]`

To return to the default values, use the `no distance weight` command.

Parameters

weight	The administrative distance value indicates the reliability of a routing information source. The range is from 1 to 255. (A higher relative value indicates lower reliability. Routes with smaller values are given preference.) The default is **115**.
ip-address mask	(OPTIONAL) Enter next-hop IP address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.

	prefix-list	(OPTIONAL) Enter the name of a prefix list name.

Defaults weight = **115**

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
6.3.1.0	Introduced.

Usage Information The administrative distance indicates the trust value of incoming packets. A low administrative distance indicates a high trust rate. A high value indicates a lower trust rate. For example, a weight of 255 is interpreted that the routing information source is not trustworthy and should be ignored.

distribute-list in

Filter network prefixes received in updates.

C9000 Series

Syntax `distribute-list` *`prefix-list-name`* `in [`*`interface`*`]`

To return to the default values, use the `no distribute-list` *`prefix-list-name`* `in [`*`interface`*`]` command.

Parameters

prefix-list-name	Specify the prefix list to filter prefixes in routing updates.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a SONET interface, enter the keyword `sonet` then the slot/port information.

- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes
- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.5.1.0	Added IPv6 ISIS support.
6.3.1.0	Introduced.

Related Commands
- distribute-list out — suppresses networks from being advertised in updates.
- redistribute — redistributes routes from one routing domain to another routing domain.

distribute-list out

Suppress network prefixes from being advertised in outbound updates.

C9000 Series

Syntax `distribute-list prefix-list-name out [connected | bgp as number | ospf process-id | rip | static]`

To return to the default values, use the `no distribute-list prefix-list-name out [bgp as number connected | ospf process-id | rip | static]` command.

Parameters

prefix-list-name	Specify the prefix list to filter prefixes in routing updates.
connected	(OPTIONAL) Enter the keyword `connected` for directly connected routing process.
ospf *process-id*	(OPTIONAL) Enter the keyword `ospf` then the OSPF process-ID number. The range is from 1 to 65535.
bgp *as number*	(OPTIONAL) Enter the BGP then the AS Number. The range is from 1 to 65535.
rip	(OPTIONAL) Enter the keyword `rip` for RIP routes.

static	(OPTIONAL) Enter the keyword `static` for user-configured routing process.

Defaults

Not configured.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
7.5.1.0	Added IPv6 ISIS support.
6.3.1.0	Introduced.

Usage Information

You can assign a name to a routing process so a prefix list IS applied to only the routes derived from the specified routing process.

Related Commands

- distribute-list in — filters the networks received in updates.
- redistribute — redistributes routes from one routing domain to another routing domain.

distribute-list redistributed-override

Suppress flapping of routes when the same route is redistributed into IS-IS from multiple routers in the network.

C9000 Series

Syntax

```
distribute-list redistributed-override in
```

To return to the default, use the `no distribute-list redistributed-override in` command.

Defaults

none

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Added IPv6 ISIS support.
6.3.1.0	Introduced.

Usage Information When you execute this command, IS-IS does not download the route to the routing table if the same route was redistributed into IS-IS routing protocol on the same router.

domain-password

Set the authentication password for a routing domain.

C9000 Series

Syntax `domain-password [hmac-md5 | encryption-type] password`

To disable the password, use the `no domain-password` command.

Parameters

hmac-md5	(OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password using MD5.
encryption-type	(OPTIONAL) Enter `7` to encrypt the password using DES.
password	Enter an alphanumeric string up to 16 characters long. If you do not specify an `encryption type` or `hmac-md5` keywords, the password is processed as plain text which provides limited security.

Defaults No default password.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
6.3.1.0	Introduced.

Usage Information The domain password is inserted in Level 2 link state PDUs (LSPs), complete sequence number PDUs (CSNPs), and partial sequence number PDUs (PSNPs).

Related Commands

- area-password — configures an IS-IS area authentication password.
- isis priority — configures the authentication password for an interface.

graceful-restart ietf

Enable graceful restart on an IS-IS router.

C9000 Series

Syntax `graceful-restart ietf`

To return to the default, use the `no graceful-restart ietf` command.

Parameters

ietf	Enter `ietf` to enable graceful restart on the IS-IS router.

Defaults Graceful restart disabled.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
6.3.1.0	Introduced on the E-Series.

Usage Information Every graceful restart enabled router's HELLO PDUs includes a restart TLV. This restart enables (re)starting as well as the existing ISIS peers to detect the GR capability of the routers on the connected network. A flag in the

Restart TLV contains restart request (RR), restart acknowledge (RA) and suppress adjacency advertisement (SA) bit flags.

The ISIS graceful restart-enabled router can co-exist in mixed topologies where some routers are graceful restart-enabled and others are not. For neighbors that are not graceful restart-enabled, the restarting router brings up the adjacency per the usual methods.

graceful-restart interval

Set the graceful restart grace period, the time during that all graceful restart attempts are prevented.

C9000 Series

Syntax

`graceful-restart interval` *minutes*

To return to the default, use the `no graceful-restart interval` command.

Parameters

minutes	Enter the graceful-restart interval minutes. The range is from 1 to 20 minutes. The default is **5 minutes**.

Defaults

5 minutes

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

graceful-restart restart-wait

Enable the graceful restart maximum wait time before a restarting peer comes up.

C9000 Series

Syntax

NOTE: Set the t3 timer to `adjacency` on the restarting router when implementing this command.

```
graceful-restart restart-wait seconds
```

To return to the default, use the `no graceful-restart restart-wait` command.

Parameters

seconds	Enter the graceful restart time in seconds. The range is from 5 to 300 seconds. The default is **30 seconds**.

Defaults **30 seconds**

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

Related Commands graceful-restart t3 — configures the overall wait time before graceful restart completes.

graceful-restart t1

Set the graceful restart wait time before unacknowledged restart requests are generated. This wait time is the interval before the system sends a restart request (an IIH with RR bit set in Restart TLV) until the CSNP is received from the helping router.

C9000 Series

Syntax

```
graceful-restart t1 {interval seconds | retry-times value}
```

To return to the default, use the `no graceful-restart t1` command.

Parameters

interval	Enter the keyword `interval` to set the wait time. The range is from 5 to 120 seconds. The default is **5 seconds**.
retry-times	Enter the keywords `retry-times` to set the number of times the request interval is extended until a CSNP is received from the helping router. The range is from 1 to 10 attempts. The default is **1**.

Defaults Refer to Parameters.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

graceful-restart t2

Configure the wait time for the graceful restart timer T2 that a restarting router uses as the wait time for each database to synchronize.

C9000 Series

Syntax `graceful-restart t2 {level-1 | level-2} seconds`

To return to the default, use the `no graceful-restart t2` command.

Parameters

level-1, level-2	Enter the keywords `level-1` or `level-2` to identify the database instance type to which the wait interval applies.
seconds	Enter the `gracefule-restart t2` time in seconds. The range is from 5 to 120 seconds. The default is **30 seconds**.

Defaults **30 seconds**

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

graceful-restart t3

Configure the overall wait time before graceful restart completes.

C9000 Series

Syntax `graceful-restart t3 {adjacency | manual}` *seconds*

To return to the default, use the `no graceful-restart t3` command.

Parameters

adjacency	Enter the keyword `adjacency` so that the restarting router receives the remaining time value from its peer and adjusts its T3 value so if you have configured this option.
manual	Enter the keyword `manual` to specify a time value that the restarting router uses. The range is from 50 to 120 seconds. The default is **30 seconds**.

Defaults manual, **30 seconds**

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

Usage Information

The running router sets the remaining time value to the current adjacency hold time. You can override this setting by implementing this command.

Override the default restart-wait time by entering the `no graceful-restart restart-wait` command. When you disable `restart-wait`, the current adjacency hold time is used.

Set the t3 timer to `adjacency` on the restarting router when implementing this command. The restarting router gets the remaining time value from its peer and adjusts its T3 value so only when you have configured `graceful-restart t3 adjacency`.

Related Commands

graceful-restart restart-wait — enables the graceful restart maximum wait time before a restarting peer comes up.

hello padding

Use to turn ON or OFF padding for LAN and point-to-point hello PDUs or to selectively turn padding ON or OFF for LAN or point-to-point hello PDUs.

C9000 Series

Syntax

`hello padding [multi-point | point-to-point]`

To return to the default, use the `no hello padding [multi-point | point-to-point]` command.

Parameters

multi-point	(OPTIONAL) Enter the keywords `multi-point` to pad only LAN hello PDUs.
point-to-point	(OPTIONAL) Enter the keywords `point-to-point` to pad only point-to-point PDUs.

Defaults

Both LAN and point-to-point hello PDUs are padded.

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Version	Description
8.3.11.1	Introduced on the Z9000.

Usage Information IS-IS hellos are padded to the full maximum transmission unit (MTU) size. Padding IS-IS Hellos (IIHS) to the full MTU provides early error detection of large frame transmission problems or mismatched MTUs on adjacent interfaces.

Related Commands isis hello padding — turns ON or OFF hello padding on an interface basis.

hostname dynamic

Enables dynamic learning of hostnames from routers in the domain and allows the routers to advertise the hostname in LSPs.

C9000 Series

Syntax `hostname dynamic`

To disable this command, use the `no hostname dynamic` command.

Defaults Enabled.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information To build name-to-systemID mapping tables through the protocol, use this command. All `show` commands that display systems also display the hostname.

Related Commands clns host — defines a name-to-NSAP mapping.

ignore-lsp-errors

Ignore LSPs with bad checksums instead of purging those LSPs.

C9000 Series

Syntax

```
ignore-lsp-errors
```

To return to the default values, use the `no ignore-lsp-errors` command.

Defaults

In IS-IS, the default deletes LSPs with internal checksum errors (`no ignore-lsp-errors`).

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

IS-IS normally purges LSPs with an incorrect data link checksum causing the LSP source to regenerate the message. A cycle of purging and regenerating LSPs can occur when a network link continues to deliver accurate LSPs even though there is a link causing data corruption. This process could cause disruption to your system operation.

ip router isis

Configure IS-IS routing processes on an interface and attach an area tag name to the routing process.

C9000 Series

Syntax

```
ip router isis [tag]
```

To disable IS-IS on an interface, use the `no ip router isis [tag]` command.

Parameters

tag	(OPTIONAL) The tag you specify identifies a specific area routing process. If you do not specify a tag, a null tag is assigned.

Defaults No processes are configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Introduced.

Usage Information To assign a network entity title to enable IS-IS, use the `net` command.

This command accepts even if an IP address is not configured. This command is cached in the L3 Manager till the IP address is configured. When the IP address configuration reaches the L3Manager, the circuit add message is sent to IS-IS.

NOTE: IP address is not mandatory for forming IS-IS adjacency.

Related Commands

- net — configures an IS-IS network entity title (NET) for the routing process.
- router isis — enables the IS-IS routing protocol.

ipv6 router isis

Enable the IPv6 IS-IS routing protocol and specify an IPv6 IS-IS process.

C9000 Series

Syntax `ipv6 router isis [tag]`

To disable IS-IS routing, use the `no router isis [tag]` command.

Parameters

tag	(OPTIONAL) This parameter is a unique name for a routing process. A null tag is assumed if the tag option is not specified. The tag name must be unique for all IP router processes for a given router.

Defaults Not configured.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Introduced on the E-Series.

Usage Information Configure a network entity title (the `net` command) to specify the area address and the router system ID.

To establish adjacencies and establish dynamic routing, enable routing on one or more interfaces.

You can configure only one IS-IS routing process to perform Level 2 routing. A `level-1-2` designation performs Level 1 and Level 2 routing at the same time.

Related Commands

- net — configures an IS-IS network entity title (NET) for the routing process.
- is-type — assigns a type for a given area.

isis circuit-type

Configure the adjacency type on interfaces.

C9000 Series

Syntax

```
isis circuit-type {level-1 | level-1-2 | level-2-only}
```

To return to the default values, use the `no isis circuit-type` command.

Parameters

level-1	You can form a Level 1 adjacency if there is at least one common area address between this system and neighbors. You cannot form Level 2 adjacencies on this interface.

level-1-2	You can form a Level 1 and Level 2 adjacencies when the neighbor is also configured as Level-1-2 and there is at least one common area, if not, a Level 2 adjacency is established. This setting is the default.
level-2-only	You can form a Level 2 adjacencies when other Level 2 or Level 1-2 routers and their interfaces are configured for Level 1-2 or Level 2. Level 1 adjacencies cannot be established on this interface.

Defaults **level-1-2**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information Because the default establishes Level 1 and Level 2 adjacencies, you do not need to configure this command. Routers in an IS-IS system must be configured as a Level 1-only, Level 1-2, or Level 2-only system.

Only configure interfaces as Level 1 or Level 2 on routers that are between areas (for example, a Level 1-2 router) to prevent the software from sending unused hello packets and wasting bandwidth.

isis csnp-interval

Configure the IS-IS complete sequence number PDU (CSNP) interval on an interface.

C9000 Series

Syntax `isis csnp-interval` *`seconds`* `[level-1 | level-2]`

To return to the default values, use the `no isis csnp-interval [`*`seconds`*`] [level-1 | level-2]` command.

Parameters

seconds	Interval of transmission time between CSNPs on multi-access networks for the designated intermediate system. The range is from 0 to 65535. The default is **10**.
level-1	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 1.

	level-2	(OPTIONAL) Independently configures the interval of time between transmission of CSNPs for Level 2.

Defaults seconds = **10**; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information The default values of this command are typically satisfactory transmission times for a specific interface on a designated intermediate system. To maintain database synchronization, the designated routers send CSNPs.

You can configure Level 1 and Level 2 CSNP intervals independently.

isis hello-interval

Specify the length of time between hello packets sent.

C9000 Series

Syntax `isis hello-interval` *`seconds`* `[level-1 | level-2]`

To return to the default values, use the `no isis hello-interval [`*`seconds`*`] [level-1 | level-2]` command.

Parameters

seconds	Allows you to set the length of time between hello packet transmissions. The range is from 1 to 65535. The default is **10**.
level-1	(OPTIONAL) Select this value to configure the hello interval for Level 1. This value is the default.
level-2	(OPTIONAL) Select this value to configure the hello interval for Level 2.

Defaults seconds = **10**; **level-1** (if not otherwise specified)

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

Hello packets are held for a length of three times the value of the hello interval. To conserve bandwidth and CPU usage, use a high hello interval seconds. Use a low hello interval seconds for faster convergence (but uses more bandwidth and CPU resources).

Related Commands

isis hello-multiplier — specifies the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency as down.

isis hello-multiplier

Specify the number of IS-IS hello packets a neighbor must miss before the router declares the adjacency down.

C9000 Series

Syntax

`isis hello-multiplier` *`multiplier`* `[level-1 | level-2]`

To return to the default values, use the `no isis hello-multiplier [`*`multiplier`*`] [level-1 | level-2]` command.

Parameters

multiplier	Specifies an integer that sets the multiplier for the hello holding time. Never configure a hello-multiplier lower than the default (3). The range is from 3 to 1000. The default is **3**.
level-1	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This value is the default.
level-2	(OPTONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.

Defaults

multiplier = **3**; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information The holdtime (the product of the hello-multiplier multiplied by the hello-interval) determines how long a neighbor waits for a hello packet before declaring the neighbor is down so routes can be recalculated.

Related Commands isis hello-interval — specifies the length of time between hello packets.

isis hello padding

Turn ON or OFF padding of hello PDUs from INTERFACE mode.

C9000 Series

Syntax `isis hello padding`

To return to the default, use the `no isis hello padding` command.

Defaults Padding of hello PDUs is enabled (ON).

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information Hello PDUs are “padded” only when both the global and interface padding options are ON. Turning either one OFF disables padding for the corresponding interface.

Related Commands hello padding — turns ON or OFF padding for LAN and point-to-point hello PDUs.

isis ipv6 metric

Assign metric to an interface for use with IPv6 information.

C9000 Series

Syntax

`isis ipv6 metric default-metric [level-1 | level-2]`

To return to the default values, use the `no ipv6 isis metric [default-metric] [level-1 | level-2]` command.

Parameters

default-metric	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 0 to 16777215. The default is **10**.
level-1	(OPTIONAL) Enter the keywords `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This value is the default.
level-2	(OPTIONAL) Enter the keywords `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults

default-metric = **10**; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Introduced on the E-Series.

Usage Information

Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis metric

Assign a metric to an interface.

C9000 Series

Syntax

`isis metric default-metric [level-1 | level-2]`

To return to the default values, use the `no isis metric [default-metric] [level-1 | level-2]` command.

Parameters

default-metric	Metric assigned to the link and used to calculate the cost from each other router via the links in the network to other destinations. You can configure this metric for Level 1 or Level 2 routing. The range is from 0 to 16777215 irrespective of the metric style. The default is **10**. If metric value is configured to more than 63, system throughs the following warning:`Warning: for metrics greater than 63, 'metric-style wide' should be configured on level-1-2, or it will be capped at 63.` If the metric style is WIDE, the metric values that are greater than 63 are only effective.
level-1	(OPTIONAL) Enter the keywords `level-1` to configure the shortest path first (SPF) calculation for Level 1 (intra-area) routing. This setting is the default.
level-2	(OPTIONAL) Enter the keywords `level-2` to configure the SPF calculation for Level 2 (inter-area) routing.

Defaults

default-metric = **10**; **level-1** (if not otherwise specified)

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information Dell Networking recommends configuring metrics on all interfaces. Without configuring this command, the IS-IS metrics are similar to hop-count metrics.

isis network point-to-point

Enable the software to treat a broadcast interface as a point-to-point interface.

C9000 Series

Syntax `isis network point-to-point`

To disable the feature, use the `no isis network point-to-point` command.

Defaults Not enabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

isis password

Configure an authentication password for an interface.

C9000 Series

Syntax `isis password [hmac-md5] password [level-1 | level-2]`

To delete a password, use the `no isis password [password] [level-1 | level-2]` command.

Parameters

encryption-type	(OPTIONAL) Enter `7` to encrypt the password using DES.
hmac-md5	(OPTIONAL) Enter the keywords `hmac-md5` to encrypt the password using MD5.
password	Assign the interface authentication password.

level-1	(OPTIONAL) Independently configures the authentication password for Level 1. The router acts as a station router for Level 1 routing. This setting is the default.
level-2	(OPTIONAL) Independently configures the authentication password for Level 2. The router acts as an area router for Level 2 routing.

Defaults No default password. **level-1** (if not otherwise specified).

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information To protect your network from unauthorized access, use this command to prevent unauthorized routers from forming adjacencies.

You can assign different passwords for different routing levels by using the keywords `level-1` and `level-2`.

The `no` form of this command disables the password for Level 1 or Level 2 routing, using the respective keywords `level-1` or `level-2`.

This password provides limited security as it is processed as plain text.

isis priority

Set the priority of the designated router you select.

C9000 Series

Syntax `isis priority value [level-1 | level-2]`

To return to the default values, use the `no isis priority [value] [level-1 | level-2]` command.

Parameters

value	This value sets the router priority. The higher the value, the higher the priority. The range is from 0 to 127. The default is **64**.
level-1	(OPTIONAL) Specify the priority for Level 1. This setting is the default.
level-2	(OPTIONAL) Specify the priority for Level 2.

Defaults value = **64**; **level-1** (if not otherwise specified).

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OSCommand Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information You can configure priorities independently for Level 1 and Level 2. Priorities determine which router on a LAN is the designated router. Priorities are advertised within hellos. The router with the highest priority becomes the designated intermediate system (DIS).

NOTE: Routers with a priority of 0 cannot be a designated router.

Setting the priority to 0 lowers the chance of this system becoming the DIS, but does not prevent it. If all the routers have priority 0, one with highest MAC address becomes DIS even though its priority is 0.

is-type

Configure IS-IS operating level for a router.

C9000 Series

Syntax `is-type {level-1 | level-1-2 | level-2-only}`

To return to the default values, use the `no is-type` command.

Parameters

level-1	Allows a router to act as a Level 1 router.
level-1-2	Allows a router to act as both a Level 1 and Level 2 router. This setting is the default.
level-2-only	Allows a router to act as a Level 2 router.

Defaults **level-1-2**

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

The IS-IS protocol automatically determines area boundaries and are able to keep Level 1 and Level 2 routing separate. Poorly planned use of this feature may cause configuration errors, such as accidental area partitioning.

If you are configuring only one area in your network, you do not need to run both Level 1 and Level 2 routing algorithms. You can configure the IS type as Level 1.

log-adjacency-changes

Generate a log messages for adjacency state changes.

C9000 Series

Syntax

`log-adjacency-changes`

To disable this function, use the `no log-adjacency-changes` command.

Defaults

Adjacency changes are not logged.

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information This command allows you to monitor adjacency state changes, which are useful when you monitor large networks. Messages are logged in the system's error message facility.

lsp-gen-interval

Set the minimum interval between successive generations of link-state packets (LSPs).

C9000 Series

Syntax `lsp-gen-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]`

To restore default values, use the `no lsp-gen-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]` command.

Parameters

level-l	(OPTIONAL) Enter the keywords `level-1` to apply the configuration to generation of Level-1 LSPs.
level-2	(OPTIONAL) Enter the keywords `level-2` to apply the configuration to generation of Level-2 LSPs.
interval seconds	Enter the maximum number of seconds between LSP generations. The range is from 0 to 120 seconds. The default is **5 seconds**.
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first LSP generation. The range is from 0 to 120 seconds. The default is **1 second**.
second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second LSP generation. The range is from 0 to 120 seconds. The default is **5 seconds**.

Defaults Refer to *Parameters*.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Added support for LSP Throttling Enhancement.

Usage Information

LSP throttling slows down the frequency at which LSPs are generated during network instability. Even though throttling LSP generations slows down network convergence, no throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of LSP generations until the topology regains its stability.

The first generation is controlled by the initial wait interval and the second generation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (`interval seconds`). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

lsp-mtu

Set the maximum transmission unit (MTU) of IS-IS link-state packets (LSPs). This command only limits the size of LSPs this router generates.

C9000 Series

Syntax

`lsp-mtu` *size*

To return to the default values, use the `no lsp-mtu` command.

Parameters

size	The maximum LSP size, in bytes. The range is from 512 to 16000 for Non-Jumbo mode and from 128 to 9195 for Jumbo mode. The default is **1497**.

NOTE: The appropriate interface circuit is brought down and removed.

Defaults

1497 bytes.

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Added support for LSP Throttling Enhancement.

Usage Information

The link MTU and the LSP MTU size must be the same.

Because each device can generate a maximum of 255 LSPs, consider carefully whether you use the `lsp-mtu` command.

lsp-refresh-interval

Set the link state PDU (LSP) refresh interval. LSPs must be refreshed before they expire. When the LSPs are not refreshed after a refresh interval, they are kept in a database until their `max-lsp-lifetime` reaches zero and then LSPs is purged.

C9000 Series

Syntax

`lsp-refresh-interval` *seconds*

To restore the default refresh interval, use the `no lsp-refresh-interval` command.

Parameters

seconds	The LSP refresh interval, in seconds. This value must be 300 seconds less than the value specified in the `max-lsp-lifetime` command. The range is from 1 to 65535 seconds. The default is **900**.

Defaults

900 seconds

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Added support for LSP Throttling Enhancement.

Usage Information

The refresh interval determines the rate at which route topology information is transmitted preventing the information from becoming obsolete.

The refresh interval must be less than the LSP lifetime specified with the `max-lsp-lifetime` command. A low value reduces the amount of time that undetected link state database corruption can persist at the cost of increased link utilization. A higher value reduces the link utilization the flooding of refreshed packets causes.

Related Commands max-lsp-lifetime — sets the maximum interval that LSPs persist without being refreshed.

max-area-addresses

Configure manual area addresses.

C9000 Series

Syntax `max-area-addresses number`

To return to the default values, use the `no max-area-addresses` command.

Parameters

number	Set the maximum number of manual area addresses. The range is from 3 to 6. The default is **3**.

Defaults **3** addresses

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.5.1.0	Added support for LSP Throttling Enhancement.

Usage Information To configure the number of area addresses on router, use this command. This value must be consistent with routers in the same area, otherwise the router forms only Level 2 adjacencies. The value must be same among all the routers to form Level 1 adjacencies.

max-lsp-lifetime

Set the maximum time that link-state packets (LSPs) exist without being refreshed.

C9000 Series

Syntax

`max-lsp-lifetime` *seconds*

To restore the default time, use the `no max-lsp-lifetime` command.

Parameters

seconds	The maximum lifetime of LSP in seconds. This value must be greater than the `lsp-refresh-interval` command. The higher the value the longer the LSPs are kept. The range is from 1 to 65535. The default is **1200**.

Defaults

1200 seconds

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

Change the maximum LSP lifetime with this command. The maximum LSP lifetime must always be greater than the LSP refresh interval.

The `seconds` parameter enables the router to keep LSPs for the specified length of time. If the value is higher, the overhead is reduced on slower-speed links.

Related Commands

lsp-refresh-interval — sets the link-state packet (LSP) refresh interval.

maximum-paths

Configure the maximum number of equal cost paths allowed in a routing table.

C9000 Series

NOTE: You can use the `maximum-paths` command to configure a single system wide value that is common for both IPv4 and IPv6 addresses.

Syntax

```
maximum-paths number
```

To return to the default values, use the `no maximum-paths` command.

Parameters

number	Enter a number as the maximum number of parallel paths an IP routing installs in a routing table. The range is from 1 to 64. The default is **4**.

Defaults

4

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Added support for multi-topology ISIS.
6.3.1.0	Introduced.

metric-style

Configure a router to generate and accept old-style, new-style, or both styles of type, length, and values (TLV).

C9000 Series

Syntax

```
metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2]
```

To return to the default values, use the `no metric-style {narrow [transition] | transition | wide [transition]} [level-1 | level-2]` command.

Parameters

narrow	Allows you to generate and accept old-style TLVs. The metric range is from 0 to 63.
transition	Allows you to generate both old-style and new-style TLVs. The metric range is from 0 to 63.
wide	Allows you to generate and accept only new-style TLVs. The metric range is from 0 to 16777215.
level-1	Enables the metric style on Level 1.
level-2	Enables the metric style on Level 2.

Defaults

narrow; if no Level is specified, Level-1 and Level-2 are configured.

Command Modes

ROUTER ISIS

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Usage Information

If you enter the `metric-style wide` command, the Dell Networking OS generates and accepts only new-style TLVs. The router uses less memory and other resources rather than generating both old-style and new-style TLVs.

The new-style TLVs have wider metric fields than old-style TLVs.

When wide transition is configured, narrow metric is sent for the narrow metric TLV and the actual wide metric is sent in wide metric TLV. The receiver can choose to use the metric that is requires.

Related Commands isis metric — configures a metric for an interface.

multi-topology

Enables multi-topology IS-IS. It also allows enabling/disabling of old and new style TLVs for IP prefix information in the LSPs.

C9000 Series

Syntax `multi-topology [transition]`

To return to a single topology configuration, use the `no multi-topology [transition]` command.

Parameters

transition

Defaults Disabled

Command Modes CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	Introduced.

net

To configure an IS-IS network entity title (NET) for a routing process, use this mandatory command. If you did not configure a NET, the IS-IS process does not start.

C9000 Series

Syntax `net network-entity-title`

To remove a net, use the `no net network-entity-title` command.

Parameters

network-entity-title	Specify the area address and system ID for an IS-IS routing process. The first 1 to 13 bytes identify the area address. The next 6 bytes identify the system ID. The last 1 byte is the selector byte, always identified as zero zero (00). This argument can be applied to an address or a name.

Defaults Not configured.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

passive-interface

Suppress routing updates on an interface. This command stops the router from sending updates on that interface.

C9000 Series

Syntax `passive-interface` *`interface`*

To delete a passive interface configuration, use the `no passive-interface` *`interface`* command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER ISIS

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information Although the passive interface does not send nor receive routing updates, the network on that interface is still included in the IS-IS updates sent using other interfaces.

redistribute

Redistribute routes from one routing domain to another routing domain.

C9000 Series

Syntax `redistribute {static | connected | rip} [level-1 | level-1-2 | level-2] [metric metric-value] [metric-type {external | internal}] [route-map map-name]`

To end redistribution or disable any of the specified keywords, use the `no redistribute {static | connected | rip} [metric metric-value] [metric-type {external | internal}] [level-1 | level-1-2 | level-2] [route-map map-name]` command.

Parameters

connected	Enter the keyword `connected` to redistribute active routes into IS-IS.
rip	Enter the keyword `rip` to redistribute RIP routes into IS-IS.
static	Enter the keyword `static` to redistribute user-configured routes into IS-IS.
metric *metric-value*	(OPTIONAL) Assign a value to the redistributed route. The range is from 0 to 16777215. The default is **0**. Use a value that is consistent with the destination protocol.
metric-type {external | internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. Specify one of the following: • `external` • `internal`
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.

level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.
route-map *map-name*	(OPTIONAL) If you do not enter the route-map argument, all routes are redistributed. If a map-name value is not specified, no routes are imported.

Defaults

- metric metric-value = **0**
- metric-type= internal; **level-2**

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.5.1.0	Added support for IPv6 ISIS.
6.3.1.0	Introduced.

Usage Information

To redistribute a default route (0.0.0.0/0), configure the `default-information originate` command.

Changing or disabling a keyword in this command does not affect the state of the other command keywords.

When an LSP with an internal metric is received, the Dell Networking OS considers the route cost while considering the advertised cost to reach the destination.

Redistributed routing information is filtered with the `distribute-list out` command to ensure that the routes are properly passed to the receiving routing protocol.

How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for Narrow or Transition mode and the metric value in the `redistribute` command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the `metric-style` command is set for Wide mode, the metric value in the `redistribute` command is advertised.

Related Commands

- default-information originate — generates a default route for the IS-IS domain.
- distribute-list out — suppresses networks from being advertised in updates. This command filters redistributed routing information.

redistribute bgp

Redistribute routing information from a BGP process.

C9000 Series

Syntax

`redistribute bgp` *`AS number`* `[level-1| level-1-2 | level-2] [metric` *`metric-value`*`] [metric-type {external| internal}] [route-map` *`map-name`*`]`

To return to the default values, use the `no redistribute bgp` command with the appropriate parameters.

Parameters

AS number	Enter a number that corresponds to the autonomous system number. The range is from 1 to 65355.
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 routes only.
level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS Level 1 and Level 2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes only. This setting is the default.
metric ***metric-value***	(OPTIONAL) The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is from 0 to 16777215. The default is **0**.
metric-type {external| internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: • `external` • `internal`
route-map ***map-name***	`map-name` is an identifier for a configured route map. The route map filters imported routes from the source routing protocol to the current routing protocol. If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

Defaults

IS-IS Level 2 routes only

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.

Version	Description
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.5.1.0	Added support for IPv6 ISIS.
6.3.1.0	Introduced.

Usage Information BGP to IS-IS redistribution supports "match" options using route maps. You can set the metric value, level, and metric-type of redistributed routes by the redistribution command. You can "set" more advanced options using route maps.

Example

```
Dell(conf)# router is
Dell(conf-router_isis)# redistribute bgp 1 level-1 metric 32 metric-type
external route-map rmap-isis-to-bgp
Dell(conf-router_bgp)#show running-config isis
!
router isis
redistribute bgp 1 level-1 metric 32 metric-type external route-map
rmap-isis-to-bgp
```

redistribute ospf

Redistribute routing information from an OSPF process.

C9000 Series

Syntax `redistribute ospf` *process-id* `[level-1| level-1-2 | level-2] [match {internal | external}] [metric` *metric-value*`] [metric-type {external | internal}] [route-map` *map-name*`]`

To return to the default values, use the `no redistribute ospf` *process-id* `[level-1| level-1-2 | level-2] [match {internal | external}] [metric` *metric-value*`][metric-type {external | internal}] [route-map` *map-name*`]` command.

Parameters

process-id	Enter a number that corresponds to the OSPF process ID to be redistributed. The range is from 1 to 65355.
metric *metric-value*	(OPTIONAL) The value used for the redistributed route. Use a metric value that is consistent with the destination protocol. The range is from 0 to 16777215. The default is **0**.
metric-type {external | internal}	(OPTIONAL) The external link type associated with the default route advertised into a routing domain. The two options are: • external • internal
level-1	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 1 routes.

level-1-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level-1-2 routes.
level-2	(OPTIONAL) Routes are independently redistributed into IS-IS as Level 2 routes. This setting is the default.
match {external | internal}	(OPTIONAL) The command used for OSPF to route and redistribute into other routing domains. The values are • `internal` • `external`
route-map *map-name*	`map-name` is an identifier for a configured route map. The route map should filter imported routes from the source routing protocol to the current routing protocol. If you do not specify a map-name, all routes are redistributed. If you specify a keyword, but fail to list route map tags, no routes are imported.

Defaults Refer to Parameters.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.5.1.0	Added support for IPv6 ISIS.
6.3.1.0	Introduced.

Usage Information How a metric value assigned to a redistributed route is advertised depends on how on the configuration of the `metric-style` command. If the `metric-style` command is set for Narrow mode and the metric value in the `redistribute ospf` command is set to a number higher than 63, the metric value advertised in LSPs is 63. If the `metric-style` command is set for wide mode, the metric value in the `redistribute ospf` command is advertised.

router isis

Enable the IS-IS routing protocol and specify an IP IS-IS process.

C9000 Series

Syntax

`router isis [tag][vrf vrf-name]`

To disable IS-IS routing, use the `no router isis [tag]` command.

Parameters

vrf *vrf-name*	Enter the keyword `vrf` followed by the name of the VRF to enable the IS-IS routing protocol and to specify an IP IS-IS process on that VRF.
tag	(OPTIONAL) This is a unique name for a routing process. A null tag is assumed if the `tag` option is not specified. The tag name must be unique for all IP router processes for a given router.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

Configure a network entity title (the `net` command) to specify the area address and the router system ID.

Enable routing on one or more interfaces to establish adjacencies and establish dynamic routing.

You can configure only one IS-IS routing process to perform Level 2 routing. A `level-1-2` designation performs Level 1 and Level 2 routing at the same time.

Related Commands

- ip router isis — configures IS-IS routing processes for IP on interfaces and attaches an area designator to the routing process.
- net — configures an IS-IS network entity title (NET) for a routing process.

- is-type — assigns a type for a given area.

set-overload-bit

Set the overload bit in zeroth fragment of non-pseudonode LSPs on the router.. This setting prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

C9000 Series

Syntax

```
set-overload-bit
```

To return to the default values, use the `no set-overload-bit` command.

Defaults

Not set.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Added support for multi-topology ISIS.
6.3.1.0	Introduced.

Usage Information

Configure the router to set the overload bit when a router experiences problems, such as a memory shortage because of an incomplete link state database. This can result in an incomplete or inaccurate routing table. If you set the overload bit in its LSPs, other routers ignore the unreliable router in their SPF calculations until the router has recovere

d.

NOTE: You can configure a single system wide value that is common for both IPv4 and IPv6 address.

show config

Display the changes you made to the IS-IS configuration. Default values are not shown.

C9000 Series

Syntax

```
show config
```

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

Example (Router-Isis)

The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.

```
Dell(conf-router_isis)# show config
!
router isis
clns host ISIS 49.0000.0001.F100.E120.0013.00
log-adjacency-changes
net 49.0000.0001.F100.E120.0013.00
!
address-family ipv6 unicast
maximum-paths 16
multi-topology transition
set-overload-bit
spf-interval level-1 100 15 20
spf-interval level-2 120 20 25
exit-address-family
```

Example (Address-Family_IPv6)

The bold section identifies that Multi-Topology IS-IS is enabled in Transition mode.

```
Dell(conf-router_isis-af_ipv6)# show conf
!
address-family ipv6 unicast
maximum-paths 16
multi-topology transition
set-overload-bit
spf-interval level-1 100 15 20
```

```
spf-interval level-2 120 20 25
exit-address-family
```

show isis database

Display the IS-IS link state database.

C9000 Series

Syntax

```
show isis database [level-1 | level-2] [local] [detail | summary] [system-id]
[lspid][vrf vrf-name]
```

Parameters

level-1	(OPTIONAL) Displays the Level 1 IS-IS link-state database.
level-2	(OPTIONAL) Displays the Level 2 IS-IS link-state database.
local	(OPTIONAL) Displays local link-state database information.
detail	(OPTIONAL) Detailed link-state database information of each LSP displays when specified. If not specified, a summary displays.
summary	(OPTIONAL) Summary of link-state database information displays when specified.
system-id	(OPTIONAL) Display link-state database for system-id.
lspid	(OPTIONAL) Display only the specified LSP.
vrf *vrf-name*	(Optional) Enter the keyword `vrf` followed by the name of the VRF to display IS-IS link state database corresponding to that VRF. **NOTE: If you do not specify this option, the IS-IS link state database corresponding to the default VRF are displayed.**

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added supported for VRF. Introduced on the S6000-ON.
9.5(0.1)	Inroduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.7.1	Introduced on the S4810.

Usage Information

The following describes the `show isis database` command shown in the following example.

Field	Description
IS-IS Level-1/ Level-2 Link State Database	Displays the IS-IS link state database for Level 1 or Level 2.
LSPID	Displays the LSP identifier. The first six octets are the System ID of the originating router. The first six octets are the System ID of the originating router. The next octet is the pseudonode ID. If this byte is not zero, the LSP describes system links. If this byte is zero (0), the LSP describes the state of the originating router. The designated router for a LAN creates and floods a pseudonode LSP and describes the attached systems. The last octet is the LSP number. An LSP is divided into multiple LSP fragments if there is more data than cannot fit in a single LSP. Each fragment has a unique LSP number. An * after the LSPID indicates that the system originates an LSP where this command was issued.
LSP Seq Num	This value is the sequence number for the LSP that allows other systems to determine if they have received the latest information from the source.
LSP Checksum	This is the checksum of the entire LSP packet.
LSP Holdtime	This value is the amount of time, in seconds, that the LSP remains valid. A zero holdtime indicates that this is a purged LSP and is being removed from the link state database. A value between brackets indicates the duration that the purged LSP stays in the database before being removed.
ATT	This value represents the Attach bit. This value indicates that the router is a Level 1-2 router and can reach other areas. Level 1-only routers and Level 1-2 routers that have lost connection to other Level 1-2 routers use the Attach bit to find the closest Level 1-2 router. They install a default route to the closest Level 1-2 router.
P	This value represents the P bit. This bit is always set to zero as Dell Networking does not support area partition repair.
OL	This value represents the overload bit, determining congestion. If the overload bit is set, other routers do not use this system as a transit router when calculating routes.

Example

The bold sections identify that MultiTopology IS-IS is enabled.

```
Dell#show isis database

IS-IS Level-1 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43    580          0/0/0

IS-IS Level-2 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x00000006 0xCF43    580          0/0/0
```

```
!
Dell#show isis database detail ISIS.00-00

IS-IS Level-1 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x0000002B 0x853B    1075         0/0/0
  Area Address: 49.0000.0001
  NLPID: 0xCC 0x8E
  IP Address: 10.1.1.1
  IPv6 Address: 1011::1
  Topology: IPv4 (0x00) IPv6 (0x8002)
  Metric: 10   IS OSPF.00
  Metric: 10   IS (MT-IPv6) OSPF.00
  Metric: 10   IP 15.1.1.0 255.255.255.0
  Metric: 10   IPv6 (MT-IPv6) 1511::/64
  Metric: 10   IPv6 (MT-IPv6) 2511::/64
  Metric: 10   IPv6 (MT-IPv6) 1011::/64
  Metric: 10   IPv6 1511::/64
  Metric: 10   IP 10.1.1.0 255.255.255.0
    Hostname: ISIS

IS-IS Level-2 Link State Database
LSPID    LSP Seq Num LSP Checksum LSP Holdtime ATT/P/OL
ISIS.00-00 * 0x0000002D 0xB2CD    1075         0/0/0
  Area Address: 49.0000.0001
  NLPID: 0xCC 0x8E
  IP Address: 10.1.1.1
  IPv6 Address: 1011::1
  Topology: IPv4 (0x00) IPv6 (0x8002)
  Metric: 10   IS OSPF.00
  Metric: 10   IS (MT-IPv6) OSPF.00
  Metric: 10   IP 10.1.1.0 255.255.255.0
  Metric: 10   IP 15.1.1.0 255.255.255.0
  Metric: 20   IP 10.3.3.0 255.255.255.0
  Metric: 10   IPv6 (MT-IPv6) 1011::/64
  Metric: 10   IPv6 (MT-IPv6) 1511::/64
  Metric: 10   IPv6 (MT-IPv6) 2511::/64
  Metric: 20   IPv6 (MT-IPv6) 1033::/64
  Metric: 10   IPv6 2511::/64
  Metric: 20   IPv6 1033::/64
  Hostname: ISIS

Dell#show isis database detail
IS-IS Level-1 Link State Database
LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime      ATT/P/OL
Dell.00-00          * 0x00000009   0x79D8        941               1/0/0
  NLPID:        0xCC
  Area Address: 49.0000.0001
```

show isis graceful-restart detail

Display detailed IS-IS graceful restart related settings.

C9000 Series

Syntax `show isis graceful-restart detail [vrf vrf-name]`

Command Modes

- EXEC
- EXEC Privilege

Parameters

vrf *vrf-name*	(Optional) Enter the keyword vrf followed by the name if the VRf to display IS-IS graceful restart details corresponding to that VRF.

NOTE: If you do not specify this option, the IS-IS graceful restart details corresponding to the default VRF are displayed.

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced on the E-Series.

Example

```
Dell#show isis graceful-restart detail
Configured Timer Value
======================
Graceful Restart    : Enabled
T3 Timer            : Manual
T3 Timeout Value    : 30
T2 Timeout Value    : 30 (level-1), 30 (level-2)
T1 Timeout Value    : 5, retry count: 1
Adjacency wait time : 30

Operational Timer Value
=======================
Current Mode/State     : Normal/RUNNING
T3 Time left           : 0
T2 Time left           : 0 (level-1), 0 (level-2)
Restart ACK rcv count  : 0 (level-1), 0 (level-2)
Restart Req rcv count  : 0 (level-1), 0 (level-2)
Suppress Adj rcv count : 0 (level-1), 0 (level-2)
Restart CSNP rcv count : 0 (level-1), 0 (level-2)
Database Sync count    : 0 (level-1), 0 (level-2)
```

show isis hostname

Display IS-IS host names configured or learned on the switch.

C9000 Series

Syntax

```
show isis hostname [vrf vrf-name]
```

Parameters

vrf *vrf-name*	Enter the keyword vrf followed by the name of the VRF to display IS-IS host names corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Example

```
Dell#show isis hostname
System Id       Dynamic Name  Static Name
*F100.E120.0013 Force10       ISIS
Dell#
```

show isis interface

Display detailed IS-IS interface status and configuration information.

C9000 Series

Syntax

```
show isis interface [interface][vrf vrf-name]
```

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a port channel interface, enter the keywords `port-channel` then a number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
vrf *vrf-name*	(OPTIONAL) Enter the keyword vrf followed by the name of the VRF to display IS-IS interface status information corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example

```
Dell>show isis int
GigabitEthernet 1/7 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 37847070, Local circuit ID 1
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
    LSP Interval: 33
GigabitEthernet 1/8 is up, line protocol is up
  MTU 1497, Encapsulation SAP
```

```
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 38371358, Local circuit ID 2
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
--More--
```

```
Dell>show isis int
TenGigabitEthernet 1/7 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 37847070, Local circuit ID 1
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
    LSP Interval: 33
TenGigabitEthernet 1/8 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 38371358, Local circuit ID 2
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
--More--
```

```
Dell>show isis int
TenGigabitEthernet 1/7/1 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 37847070, Local circuit ID 1
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.01
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-2 adjacencies: 1
    Next IS-IS LAN Level-1 Hello in 2 seconds
    Next IS-IS LAN Level-2 Hello in 1 seconds
    LSP Interval: 33
TenGigabitEthernet 1/8/1 is up, line protocol is up
  MTU 1497, Encapsulation SAP
  Routing Protocol: IS-IS
    Circuit Type: Level-1-2
    Interface Index 38371358, Local circuit ID 2
    Level-1 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
    Number of active level-1 adjacencies: 1
    Level-2 Metric: 10, Priority: 64, Circuit ID: systest-3.02
     Hello Interval: 10, Hello Multiplier: 3, CSNP Interval: 10
--More--
```

show isis neighbors

Display information about neighboring (adjacent) routers.

C9000 Series

Syntax `show isis neighbors [level-1 | level-2] [detail] [interface][vrf vrf-name]`

Parameters

level-1	(OPTIONAL) Displays information about Level 1 IS-IS neighbors.
level-2	(OPTIONAL) Displays information about Level 2 IS-IS neighbors.
detail	(OPTIONAL) Displays detailed information about neighbors.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf`followed by the name of the VRF to display adjacent router information corresponding to that VRF

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.

Usage Information

Use this command to confirm that the neighbor adjacencies are operating correctly. If you suspect that they are not, you can verify the specified area addresses of the routers by using the `show isis neighbors` command.

The following describes the `show isis neighbors` command shown in the following example.

Field	Description
System Id	The value that identifies a system in an area.
Interface	The interface, slot, and port in which the router was discovered.
State	The value providing status about the adjacency state. The range is Up and Init.
Type	This value displays the adjacency type (Layer 2, Layer 2 or both).
Priority	IS-IS priority the neighbor advertises. The neighbor with highest priority becomes the designated router for the interface.
Uptime	Displays the interfaces uptime.
Circuit Id	The neighbor's interpretation of the designated router for the interface.

Example

The bold sections below identify that Multi-Topology IS-IS is enabled. This command displays only one IP address per line.

```
Dell#show isis neighbors
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2(M) 127 09:28:01 TEST.02
!
Dell#show isis neighbors detail
System Id Interface State Type Priority Uptime Circuit Id
TEST Gi 7/1 Up L1L2(M) 127 09:28:04 TEST.02 Area Address(es):
49.0000.0001
  IP Address(es): 25.1.1.3*
  MAC Address: 0000.0000.0000
  Hold Time: 28
  Link Local Address: fe80::201:e8ff:fe00:492c
  Topology: IPv4 IPv6 , Common (IPv4 IPv6 )
  Adjacency being used for MTs: IPv4 IPv6
Dell#
```

```
Dell#show isis neighbors
System Id Interface State Type Priority Uptime Circuit Id
TEST Te 7/1 Up L1L2(M) 127 09:28:01 TEST.02
!
Dell#show isis neighbors detail
System Id Interface State Type Priority Uptime Circuit Id
TEST Te 7/1 Up L1L2(M) 127 09:28:04 TEST.02 Area Address(es):
49.0000.0001
  IP Address(es): 25.1.1.3*
  MAC Address: 0000.0000.0000
  Hold Time: 28
  Link Local Address: fe80::201:e8ff:fe00:492c
  Topology: IPv4 IPv6 , Common (IPv4 IPv6 )
  Adjacency being used for MTs: IPv4 IPv6
Dell#
```

```
Dell#show isis neighbors
System Id Interface State Type Priority Uptime Circuit Id
TEST Te 7/1/1 Up L1L2(M) 127 09:28:01 TEST.02
!
Dell#show isis neighbors detail
System Id Interface State Type Priority Uptime Circuit Id
TEST Te 7/1/1 Up L1L2(M) 127 09:28:04 TEST.02 Area Address(es):
49.0000.0001
  IP Address(es): 25.1.1.3*
  MAC Address: 0000.0000.0000
```

```
  Hold Time: 28
  Link Local Address: fe80::201:e8ff:fe00:492c
  Topology: IPv4 IPv6 , Common (IPv4 IPv6 )
  Adjacency being used for MTs: IPv4 IPv6
Dell#
```

show isis protocol

Display IS-IS routing information.

C9000 Series

Syntax

```
show isis protocol [vrf vrf-name]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to display IS-IS routing information corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example

The bold section identifies that Multi-Topology IS-IS is enabled.

```
Dell#show isis protocol
IS-IS Router: <Null Tag>
  System Id: F100.E120.0013 IS-Type: level-1-2
  Manual area address(es):
   49.0000.0001
  Routing for area address(es):
   49.0000.0001
  Interfaces supported by IS-IS:
  GigabitEthernet 1/1 - IP - IPv6
  GigabitEthernet 1/2 - IP - IPv6
  GigabitEthernet 1/10 - IP - IPv6
  Loopback 0 - IP - IPv6
```

```
Redistributing:
Distance: 115
Generate narrow metrics: level-1-2
Accept narrow metrics:   level-1-2
Generate wide metrics:   none
Accept wide metrics:     none
Multi Topology Routing is enabled in transition mode.
Dell#
```

```
Dell#show isis protocol
IS-IS Router: <Null Tag>
  System Id: F100.E120.0013 IS-Type: level-1-2
  Manual area address(es):
   49.0000.0001
  Routing for area address(es):
   49.0000.0001
  Interfaces supported by IS-IS:
  TenGigabitEthernet 1/1 - IP - IPv6
  TenGigabitEthernet 1/2 - IP - IPv6
  TenGigabitEthernet 1/10 - IP - IPv6
  Loopback 0 - IP - IPv6
Redistributing:
Distance: 115
Generate narrow metrics: level-1-2
Accept narrow metrics:   level-1-2
Generate wide metrics:   none
Accept wide metrics:     none
Multi Topology Routing is enabled in transition mode.
Dell#
```

```
Dell#show isis protocol
IS-IS Router: <Null Tag>
  System Id: F100.E120.0013 IS-Type: level-1-2
  Manual area address(es):
   49.0000.0001
  Routing for area address(es):
   49.0000.0001
  Interfaces supported by IS-IS:
  TenGigabitEthernet 1/1/1 - IP - IPv6
  TenGigabitEthernet 1/2/1 - IP - IPv6
  TenGigabitEthernet 1/10/1 - IP - IPv6
  Loopback 0 - IP - IPv6
Redistributing:
Distance: 115
Generate narrow metrics: level-1-2
Accept narrow metrics:   level-1-2
Generate wide metrics:   none
Accept wide metrics:     none
Multi Topology Routing is enabled in transition mode.
Dell#
```

show isis traffic

This command allows you to display IS-IS traffic interface information.

C9000 Series

Syntax `show isis traffic [interface][vrf vrf-name]`

Parameters

interface (OPTIONAL) Identifies the interface type slot/port as one of the following:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

vrf *vrf-name* (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to display IS-IS traffic interface information corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Information

The following describes the `show isis traffic` command shown in the following example.

Item	Description
Level-1/Level-2 Hellos (sent/rcvd)	Displays the number of Hello packets sent and received.
PTP Hellos (sent/rcvd)	Displays the number of point-to-point Hellos sent and received.
Level-1/Level-2 LSPs sourced (new/refresh)	Displays the number of new and refreshed LSPs.
Level-1/Level-2 LSPs flooded (sent/rcvd)	Displays the number of flooded LSPs sent and received.
Level-1/Level-2 LSPs CSNPs (sent/rcvd)	Displays the number of CSNP LSPs sent and received.

Item	Description
Level-1/Level-2 LSPs PSNPs (sent/ rcvd)	Displays the number of PSNP LPSs sent and received.
Level-1/Level-2 DR Elections	Displays the number of times designated router elections ran.
Level-1/Level-2 SPF Calculations	Displays the number of shortest path first calculations.
LSP checksum errors received	Displays the number of checksum errors LSPs received.
LSP authentication failures	Displays the number of LSP authentication failures.

Example

```
Dell#show is traffic
  IS-IS: Level-1 Hellos (sent/rcvd) : 0/721
  IS-IS: Level-2 Hellos (sent/rcvd) : 900/943
  IS-IS: PTP Hellos (sent/rcvd) : 0/0
  IS-IS: Level-1 LSPs sourced (new/refresh) : 0/0
  IS-IS: Level-2 LSPs sourced (new/refresh) : 1/3
  IS-IS: Level-1 LSPs flooded (sent/rcvd) : 0/0
  IS-IS: Level-2 LSPs flooded (sent/rcvd) : 5934/5217
  IS-IS: Level-1 LSPs CSNPs (sent/rcvd) : 0/0
  IS-IS: Level-2 LSPs CSNPs (sent/rcvd) : 472/238
  IS-IS: Level-1 LSPs PSNPs (sent/rcvd) : 0/0
  IS-IS: Level-2 LSPs PSNPs (sent/rcvd) : 10/337
  IS-IS: Level-1 DR Elections : 4
  IS-IS: Level-2 DR Elections : 4
  IS-IS: Level-1 SPF Calculations : 0
  IS-IS: Level-2 SPF Calculations : 389
  IS-IS: LSP checksum errors received : 0
  IS-IS: LSP authentication failures : 0
Dell#
```

spf-interval

Specify the minimum interval between shortest path first (SPF) calculations.

C9000 Series

Syntax

`spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]`

To restore default values, use the `no spf-interval [level-1 | level-2] interval seconds [initial_wait_interval seconds [second_wait_interval seconds]]` command.

Parameters

level-1	(OPTIONAL) Enter the keyword `level-1` to apply the configuration to Level-1 SPF calculations.
level-2	(OPTIONAL) Enter the keyword `level-2` to apply the configuration to Level-2 SPF calculations.

interval seconds	Enter the maximum number of seconds between SPF calculations. The range is from 0 to 120 seconds. The default is **10 seconds**.
initial_wait_interval seconds	(OPTIONAL) Enter the initial wait time, in seconds, before running the first SPF calculations. The range is from 0 to 120 seconds. The default is **5 seconds**.
second_wait_interval seconds	(OPTIONAL) Enter the wait interval, in seconds, between the first and second SPF calculations. The range is from 0 to 120 seconds. The default is **5 seconds**.

Defaults

Refer to *Parameters*.

Command Modes

- ROUTER ISIS (*for IPv4*)
- CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (*for IPv6*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	Added support for multi-topology ISIS.
7.5.1.0	Added support for SPF Throttling Enhancement.

Usage Information

This command `spf-interval` in CONFIG-ROUTER-ISIS-AF-IPV6 mode is used for IPv6 Multi-Topology route computation only. If using Single Topology mode, use the `spf-interval` command in CONFIG-ROUTER-ISIS mode for both IPv4 and IPv6 route computations.

SPF throttling slows down the frequency at which route calculations are performed during network instability. Even though throttling route calculations slows down network convergence, not throttling can result in a network not functioning as expected. If network topology is unstable, throttling slows down the scheduling of route calculations until the topology regains its stability.

The first route calculation is controlled by the initial wait interval and the second calculation is controlled by the second wait interval. Each subsequent wait interval is twice as long as the previous one until the wait interval reaches the maximum wait time specified (`interval seconds`). After the network calms down and there are no triggers for two times the maximum interval, fast behavior is restored (the initial wait time).

24

Internet Group Management Protocol (IGMP)

IGMP and IGMP snooping commands are supported by the Dell Networking OS on the switch.

This chapter contains the following sections:

- IGMP Commands
- IGMP Snooping Commands

Topics:

- IGMP Commands
- IGMP Snooping Commands

IGMP Commands

The system supports IGMPv1/v2/v3 and is compliant with RFC-3376.

Important Points to Remember

- The system supports protocol-independent multicast-sparse (PIM-SM) and protocol-independent source-specific multicast (PIM-SSM) include and exclude modes.
- IGMPv2 is the default version of IGMP on interfaces. You can configure IGMPv3 on interfaces. It is backward compatible with IGMPv2.
- The switch supports up to 95 interfaces.
- There is no hard limit on the maximum number of groups supported.
- IGMPv3 router interoperability with IGMPv2 and IGMPv1 routers on the same subnet is not supported.
- An administrative command (`ip igmp version`) is added to manually set the IGMP version.
- All commands previously used for IGMPv2 are compatible with IGMPv3.

clear ip igmp groups

Clear entries from the group cache table.

C9000 Series

Syntax `clear ip igmp groups [group-address | interface]`

Parameters

group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface *interface*	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number.

- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

debug ip igmp

Enable debugging of IGMP packets.

C9000 Series

Syntax `debug ip igmp [group address | interface]`

- To disable IGMP debugging, use the `no debug ip igmp [group address | interface]` command.
- To disable all debugging, use the `undebug all` command.

Parameters

group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface *interface*	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number.

Defaults Disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information IGMP commands accept *only* non-VLAN interfaces — specifying VLAN does not yield results. This command displays packets for IGMP and IGMP snooping.

ip igmp access-group

Specify access control list for packets in access-group.

C9000 Series

Syntax `ip igmp access-group` *`access-list`*

To remove the feature, use the `no ip igmp access-group access-list` command.

Parameters

access-list	Enter the name of the extended ACL (16 characters maximum).

Defaults Not configured

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Version	Description
7.6.1.0	Introduced on the E-Series.

Usage Information The access list accepted is an extended ACL. The `ip igmp access-group` command allows you to block IGMP reports from hosts, on a per-interface basis based on the group address and source address that you specify in the access list.

ip igmp group-join-limit

Set a limit to the number of IGMP groups that can be joined in a second,

C9000 Series

Syntax `ip igmp group-join-limit number`

Parameters

number	Enter the number of IGMP groups permitted to join in a second. The range is from 1 to 10000.

Defaults none

Command Modes CONFIGURATION (conf-if-*interface-slot/port*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.
7.6.1.0	Introduced on the E-Series.

ip igmp immediate-leave

Enable IGMP immediate leave.

C9000 Series

Syntax

`ip igmp immediate-leave [group-list prefix-list-name]`

To disable `ip igmp immediate leave`, use the `no ip igmp immediate-leave` command.

Parameters

group-list *prefix-list-name*	Enter the keywords `group-list` then a string up to 16 characters long of the prefix-list-name.

Defaults

Not configured.

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.

Usage Information

Querier normally sends some group-specific queries when a `leave` message is received for a group prior to deleting a group from the membership database. There may be situations when you require immediate deletion of a group from the membership database. This command provides a way to achieve the immediate deletion. In addition, this command provides a way to enable `immediate-leave processing` for specified groups.

ip igmp last-member-query-interval

Change the last member query interval, which is the Max Response Time inserted into Group-Specific Queries sent in response to Leave Group messages. This interval is also the interval between Group-Specific Query messages.

C9000 Series

Syntax

`ip igmp last-member-query-interval` *`milliseconds`*

To return to the default value, use the `no ip igmp last-member-query-interval` command.

Parameters

milliseconds	Enter the number of milliseconds as the interval. For IGMP version 2, the range is from 100 to 25599. For IGMP version 3, the range is from 100 to 65535. The default value is **1000 milliseconds**.

Defaults

1000 milliseconds

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. For IGMP version 2, the Interval range is modified.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
E-Series legacy command	

ip igmp querier-timeout

Change the interval that must pass before a multicast router decides that there is no longer another multicast router that should be the querier.

C9000 Series

Syntax

`ip igmp querier-timeout` *seconds*

To return to the default value, use the `no ip igmp querier-timeout` command.

Parameters

seconds	Enter the number of seconds the router must wait to become the new querier. The range is from 60 to 300. The default is **125 seconds**.

Defaults

125 seconds

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
7.5.1.0	Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

ip igmp query-interval

Change the transmission frequency of IGMP general queries the Querier sends.

C9000 Series

Syntax

`ip igmp query-interval seconds`

To return to the default values, use the `no ip igmp query-interval` command.

Parameters

seconds	Enter the number of seconds between queries sent out. The range is from 1 to 18000. The default is **60 seconds**.

Defaults

60 seconds

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Maximum range of the Hello interval value is changed to 18000.
9.5(0.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
7.5.1.0	Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

Version	Description
E-Series legacy command.	

Usage Information

If you have configured the hello interval value to be greater than 18000, you must first reset that value to be less than or equal to 18000 before upload. Otherwise, the command execution fails during bootup and the hello interval value is set to the default value.

ip igmp query-max-resp-time

Set the maximum query response time advertised in general queries.

C9000 Series

Syntax

`ip igmp query-max-resp-time` *seconds*

To return to the default values, use the `no ip igmp query-max-resp-time` command.

Parameters

seconds	Enter the number of seconds for the maximum response time. The range is from 1 to 25. The default is **10 seconds**.

Defaults

10 seconds

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
7.6.1.0	Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.
7.5.1.0	Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.

ip igmp ssm-map

To translate (*,G) memberships to (S,G) memberships, use a statically configured list.

C9000 Series

Syntax

`ip igmp ssm-map` *`std-access-list source-address`*

Undo this configuration, that is, remove SSM map (S,G) states and replace them with (*,G) state, use the `ip igmp ssm-map` *`std-access-list source-address`* command.

Parameters

std-access-list	Specify the standard IP access list that contains the mapping rules for multicast groups.
source-address	Specify the multicast source address to which the groups are mapped.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
Version 9.5(0.0)	Introduced on the Z9500.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 7.8.1.0	Introduced on the C-Series and S-Series.
Version 7.7.1.0	Introduced on the E-Series.

Usage Information

Mapping applies to both v1 and v2 IGMP joins; any updates to the ACL are reflected in the IGMP groups. You may not use extended access lists with this command. When you configure a static SSM map and the router cannot find any matching access lists, the router continues to accept (*,G) groups.

Related Commands

ip access-list standard — creates a standard access list to filter based on IP address.

ip igmp static-group

Configure an IGMP static group.

C9000 Series

Syntax

`ip igmp static-group {group address [exclude [source address]] | [include {source address}]}`

To delete a static address, use the `no ip igmp static-group {group address [exclude [source address]] | [include {source address}]}` command.

Parameters

group address	Enter the group address in dotted decimal format (A.B.C.D).
exclude *source address*	(OPTIONAL) Enter the keyword `exclude` then the source address, in dotted decimal format (A.B.C.D), for which a static entry is added.
include *source address*	(OPTIONAL) Enter the keyword `include` then the source address, in dotted decimal format (A.B.C.D), for which a static entry is added.

Defaults

none

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Expanded to support the `exclude` and `include` options.

Usage Information

A group in `include` mode must have at least one source address defined. In `exclude` mode, if you do not specify a source address, The system implicitly assumes all sources are included. If you do not specify either `include` or `exclude`, the system implicitly assumes a IGMPv2 static join.

Command Limitations

- Only one mode (`include` or `exclude`) is permitted per multicast group per interface. To configure another mode, all sources belonging to the original mode must be unconfigured.

- If a static configuration is present and a packet for the same group arrives on an interface, the dynamic entry completely overwrites all the static configuration for the group.

Related Commands show ip igmp groups — displays IGMP group information.

ip igmp version

Manually set the version of the router to IGMPv2 or IGMPv3.

C9000 Series

Syntax `ip igmp version {2 | 3}`

Parameters

2	Enter the number 2 to set the IGMP version number to IGMPv2.
3	Enter the number 3 to set the IGMP version number to IGMPv3.

Defaults **2** (that is, IGMPv2)

Command Modes INTERFACE

INTERFACE (BATCH Mode)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Changed the default IGMP from version 2 to version 3.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

show ip igmp groups

View the IGMP groups.

C9000 Series

Syntax

```
show ip igmp groups [group-address [detail] | detail | interface [group-address [detail]]]
```

Parameters

group-address	(OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.
interface	(OPTIONAL) Enter the interface type and slot/port information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a port channel interface, enter the keywords `port-channel` then a number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
detail	(OPTIONAL) Enter the keyword `detail` to display the IGMPv3 source information.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series and C-Series.
7.5.1.0	Expanded to support the `detail` option.
E-Series legacy command.	

Usage Information

This command displays the IGMP database, including configured entries for either all groups on all interfaces, all groups on specific interfaces, or specific groups on specific interfaces.

The following describes the `show ip igmp groups` command shown in the following example.

Field	Description
Group Address	Lists the multicast address for the IGMP group.
Interface	Lists the interface type, slot and port number.
Mode	Displays the IGMP version used.
Uptime	Displays the amount of time the group has been operational.
Expires	Displays the amount of time until the entry expires.
Last Reporter	Displays the IP address of the last host to be a member of the IGMP group.

Example

```
Dell#show ip igmp groups
Total Number of Groups: 5
IGMP Connected Group Membership
Group Address Interface Uptime   Expires
225.0.0.0    Vlan 100   00:00:05 00:02:04

225.0.0.1    Vlan 100   00:00:05 00:02:04

225.0.0.2    Vlan 100   00:00:05 00:02:04

225.0.0.3    Vlan 100   00:00:05 00:02:04

225.0.0.4    Vlan 100   00:00:05 00:02:04
```

Example (VLT)

NOTE: The asterisk (*) after the port channel number (Po 2) highlighted in the following example indicates that the port channel is VLT, that the local VLT port channel is down and the remote VLT port is up.

```
Dell#show ip igmp groups
Total Number of Groups: 5
IGMP Connected Group Membership
Group Address Interface Mode Uptime Expires Last Reporter
225.0.0.0    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51

225.0.0.1    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51

225.0.0.2    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51

225.0.0.3    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51

225.0.0.4    Vlan 100 IGMPv2 00:00:05 00:02:04 3.0.0.51
```

Example (Details)

```
Dell#show ip igmp group details
Interface                  Vlan 20
Group                         232.1.1.5
Uptime                       00:11:22
Expires                        Never
Router mode             INCLUDE
Last reporter             35.0.0.2
Group source list
Source address           Expires
65.0.0.1                          00:01:22
65.0.0.2                          00:01:22
65.0.0.3                          00:01:22
65.0.0.4                          00:01:22
65.0.0.5                          00:01:22
```

show ip igmp interface

View information on the interfaces participating in IGMP.

C9000 Series

Syntax

```
show ip igmp interface [interface]
```

Parameters

interface (OPTIONAL) Enter the interface type and slot/port information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command.	

Usage Information

IGMP commands accept *only* non-VLAN interfaces — specifying VLAN does not yield results.

The `show ip igmp interface` command does not display information corresponding to the loop-back interfaces.

Example

```
Dell#show ip igmp interface
GigabitEthernet 0/0 is down, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 0/5 is down, line protocol is down
  Internet protocol processing disabled
```

```
GigabitEthernet 0/6 is down, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 0/7 is up, line protocol is down
  Internet protocol processing disabled
GigabitEthernet 7/9 is up, line protocol is up
  Internet address is 10.87.5.250/24
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  IGMP querier timeout is 120 seconds
  IGMP max query response time is 10 seconds
  IGMP last member query response interval is 1000 ms
  IGMP activity: 0 joins, 0 leaves
  IGMP querying router is 10.87.5.250 (this system)
  IGMP version is 2
```

show ip igmp ssm-map

Display is a list of groups that are currently in the IGMP group table and contain SSM mapped sources.

C9000 Series

Syntax

```
show ip igmp ssm-map [group]
```

Parameters

group	(OPTIONAL) Enter the multicast group address in the form A.B.C.D to display the list of sources to which this group is mapped.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.
7.7.1.0	Introduced on the E-Series.

Example

```
Dell#show ip igmp ssm-map
Interface                   Vlan 20
Group                          232.1.1.5
Uptime                        00:11:22
Expires                         Never
Router mode              INCLUDE
Last reporter               35.0.0.2
```

```
Group source list
Source address          Expires
65.0.0.1                        00:01:22
65.0.0.2                        00:01:22
65.0.0.3                        00:01:22
65.0.0.4                        00:01:22
65.0.0.5                        00:01:22
```

Related Commands ip igmp ssm-map — uses a statically configured list to translate (*,G) memberships to (S,G) memberships.

IGMP Snooping Commands

IGMP Snooping version 2 and 3 are supported on the switch.

Important Points to Remember for IGMP Snooping

- The Dell Networking OS supports version 1, version 2, and version 3 hosts.
- The IGMP snooping implementation is based on IP multicast address (not based on Layer 2 multicast mac address) and the IGMP snooping entries are in Layer 3 flow table not in Layer 2 forwarding information base (FIB).
- The IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- The system supports IGMP snooping on JUMBO-enabled cards.
- IGMP snooping is not enabled by default on the switch.
- A maximum of 1800 groups and 600 VLAN are supported.
- IGMP snooping is not supported on a default VLAN interface.
- IGMP snooping is not supported over VLAN-Stack-enabled VLAN interfaces (you must disable IGMP snooping on a VLAN interface before configuring VLAN-Stack-related commands).
- IGMP snooping does not react to Layer 2 topology changes triggered by spanning tree protocol (STP).
- IGMP snooping reacts to Layer 2 topology changes multiple spanning tree protocol (MSTP) triggers by sending a general query on the interface that comes in the FWD state.

Important Points to Remember for IGMP Querier

- The IGMP snooping Querier supports version 2.
- You must configure an IP address to the VLAN interface for IGMP snooping Querier to begin. The IGMP snooping Querier disables itself when a VLAN IP address is cleared, and then it restarts itself when an IP address is reassigned to the VLAN interface.
- When enabled, IGMP snooping Querier does not start if there is a statically configured multicast router interface in the VLAN.
- When enabled, IGMP snooping Querier starts after one query interval in case no IGMP general query (with IP SA lower than its VLAN IP address) is received on any of its VLAN members.
- When enabled, IGMP snooping Querier periodically sends general queries with an IP source address of the VLAN interface. If it receives a general query on any of its VLAN member, it checks the IP source address of the incoming frame.

  If the IP SA in the incoming IGMP general query frame is lower than the IP address of the VLAN interface, the switch disables its IGMP snooping Querier functionality.

  If the IP SA of the incoming IGMP general query is higher than the VLAN IP address, the switch continues to work as an IGMP snooping Querier.

clear ip igmp snooping groups

Clear snooping entries from the group cache table.

C9000 Series

Syntax `clear ip igmp snooping groups [group-address interface | interface]`

Parameters

group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface *interface*	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on S-Series and Z–Series.

Usage Information IGMP commands accept only non-VLAN interfaces — specifying VLAN does not yield results.

debug ip igmp snooping

Enable debugging of IGMP snooping packets on interfaces and groups.

C9000 Series

Syntax `debug ip igmp snooping [group address | interface]`

- To disable debugging of IGMP snooping, use the `no debug ip igmp snooping [group address | interface]` command.
- To disable all debugging, use the `undebug all` command.

Parameters

snooping	Enter the keyword snooping to enable debugging of IGMP snooping.
group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface *interface*	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number.

Defaults Disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, Z9000, and Z9500.

Usage Information IGMP commands accept *only* non-VLAN interfaces — specifying VLAN does not yield results. This command displays packets for IGMP and IGMP snooping.

ip igmp snooping enable

Enable IGMP snooping on all or a single VLAN. This command is the master on/off switch to enable IGMP snooping.

C9000 Series

Syntax `ip igmp snooping enable`

To disable IGMP snooping, use the `no ip igmp snooping enable` command.

Defaults Disabled.

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

To enable IGMP snooping, enter this command. When you enable this command from CONFIGURATION mode, IGMP snooping enables on all VLAN interfaces (except the default VLAN). Use this command in Configuration Terminal Batch mode to enable IGMP snooping in a dual-homing setup.

NOTE: Execute the `no shutdown` command on the VLAN interface for IGMP Snooping to function.

ip igmp snooping fast-leave

Enable IGMP snooping fast-leave for this VLAN.

C9000 Series

Syntax

```
ip igmp snooping fast-leave
```

To disable IGMP snooping fast leave, use the `no igmp snooping fast-leave` command.

Defaults

Not configured.

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

Queriers normally send some queries when a leave message is received prior to deleting a group from the membership database. There may be situations when you require a fast deletion of a group. When you enable IGMP fast leave processing, the switch removes an interface from the multicast group as soon as it detects an IGMP version 2 leave message on the interface.

ip igmp snooping flood

Control the flooding behavior of unregistered multicast data packets.

C9000 Series

Syntax

```
ip igmp snooping flood
```

Defaults

Enabled.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Seris and S-Series.
7.7.1.0	Introduced on the E-Series.

Usage Information

On the C-Series and S-Series, unregistered multicast data traffic drops when you disable flooding; they do not forward the packets to multicast router ports. On the C-Series and S-Series, in order to disable Layer 2 multicast flooding, disable Layer 3 multicast (`no ip multicast-routing`).

Use this command in Configuration Terminal Batch mode to control the flooding behavior in a dual-homing setup.

ip igmp snooping last-member-query-interval

The last member query interval is the maximum response time inserted into Group-Specific queries sent in response to Group-Leave messages.

C9000 Series

Syntax

`ip igmp snooping last-member-query-interval` *`milliseconds`*

To return to the default value, use the `no ip igmp snooping last-member-query-interval` command.

Parameters

milliseconds	Enter the interval in milliseconds. The range is from 100 to 65535. The default is **1000 milliseconds**.

Defaults

1000 milliseconds

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

The last-member-query-interval is also the interval between successive Group-Specific Query messages. The `ip igmp snooping last-member-query-interval` command allows you to change the last-member-query interval.

ip igmp snooping mrouter

Statically configure a VLAN member port as a multicast router interface.

C9000 Series

Syntax

`ip igmp snooping mrouter interface` *`interface`*

To delete a specific multicast router interface, use the `no igmp snooping mrouter interface` *`interface`* command.

Parameters

interface ***interface***

Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. For the C-Series and S-Series, the range is from 1 to 128.

Defaults

Not configured.

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information Dell Networking OS provides the capability of statically configuring the interface to which a multicast router is attached. To configure a static connection to the multicast router, enter the `ip igmp snooping mrouter interface` command in the VLAN context. The interface to the router must be a part of the VLAN where you are entering the command.

ip igmp snooping querier

Enable IGMP querier processing for the VLAN interface.

C9000 Series

Syntax `ip igmp snooping querier`

To disable IGMP querier processing for the VLAN interface, use the `no ip igmp snooping querier` command.

Defaults Not configured.

Command Modes INTERFACE

INTERFACE (BATCH Mode)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

This command enables the IGMP switch to send General Queries periodically. This behavior is useful when there is no multicast router present in the VLAN because the multicast traffic is not routed. Assign an IP address to the VLAN interface for the switch to act as a querier for this VLAN.

show ip igmp snooping mrouter

Display multicast router interfaces.

C9000 Series

Syntax

```
show ip igmp snooping mrouter [vlan number]
```

Parameters

vlan *number*	Enter the keyword `vlan` then the vlan number. The range is from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

If the port channel is a VLT port channel, an asterisk (*) after the port channel number (Po 100*) indicates the port channel is locally down and that a remote VLT port is up.

Example

```
Dell#show ip igmp snooping mrouter
Interface Router Ports
Vlan 2 Te 1/3, Po 1
Dell#
```

Related Commands

- ip igmp snooping mrouter — configures a static connection to the multicast router.
- show ip igmp groups — view groups.

show ip igmp snooping groups

Display snooping related information for all the IGMP groups and interfaces or a single group belonging to a specified interface.

C9000 Series

Syntax

```
show ip igmp snooping groups [group-address [detail] | detail | interface
[group-address [detail]]]
```

Parameters

snooping	Enter the keyword `snooping` to display snooping related information.
group-address	(OPTIONAL) Enter the group address in dotted decimal format to view information on that group only.
interface	(OPTIONAL) Enter the interface type and slot/port information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a port channel interface, enter the keywords `port-channel` then a number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094. • For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.
detail	(OPTIONAL) Enter the keyword `detail` to display the IGMPv3 source information.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, Z9000, and Z9500.

Usage Information

This command displays the IGMP database, including configured entries for either all groups on all interfaces, all groups on specific interfaces, or specific groups on specific interfaces.

The following describes the `show ip igmp groups` command shown in the following example.

Field	Description
Group Address	Lists the multicast address for the IGMP group.
Interface	Lists the interface type, slot and port number.
Mode	Displays the IGMP version used.
Uptime	Displays the amount of time the group has been operational.
Expires	Displays the amount of time until the entry expires.
Last Reporter	Displays the IP address of the last host to be a member of the IGMP group.
Member Ports	Indicates the port channel. If the port channel is VLT, an asterisk (*) after the port channel number indicates the port channel is locally down and that a remote VLT port is up.

Example

```
Dell#show ip igmp snooping groups
Total Number of Groups: 1
IGMP Connected Group Membership
Group Address    Interface      Mode          Uptime    Expires   Last Reporter
225.1.1.1        Vlan 10       IGMPv2-Compat  00:00:07  00:02:09  1.1.1.2
  Member Ports: Te 1/17
Dell#
```

```
Dell#show ip igmp snooping groups
Total Number of Groups: 1
IGMP Connected Group Membership
Group Address    Interface      Mode          Uptime    Expires   Last Reporter
225.1.1.1        Vlan 10       IGMPv2-Compat  00:00:07  00:02:09  1.1.1.2
  Member Ports: Gi 1/17
Dell#
```

```
Dell#show ip igmp snooping groups
Total Number of Groups: 1
IGMP Connected Group Membership
Group Address    Interface      Mode          Uptime    Expires   Last Reporter
225.1.1.1        Vlan 10       IGMPv2-Compat  00:00:07  00:02:09  1.1.1.2
  Member Ports: Te 1/17/1
Dell#
```

25

Internet Protocol Security (IPSec)

Internet protocol security (IPSec) is an end-to-end security scheme for securing IP communications by authenticating and encrypting all packets in a session. Use IPSec between hosts, gateways, or hosts and gateways.

IPSec uses a series of protocol functions to achieve information security:

- **Authentication Headers (AH)** — connectionless integrity and origin authentication for IP packets.
- **Encapsulating Security Payloads (ESP)** — confidentiality, authentication, and data integrity for IP packets.
- **Security Associations (SA)** — algorithm-provided parameters required for AH and ESP protocols.

IPSec capability is available on control (protocol) and management traffic; end-node support is required.

IPSec supports two operational modes: Transport and Tunnel.

- Transport is the default mode for IPSec and encrypts only the payload of the packet. Routing information is unchanged.
- Tunnel mode is used to encrypt the entire packet, including the routing information in the IP header. Tunnel mode is typically used in creating virtual private networks (VPNs).

Transport mode provides IP packet payload protection using ESP. You can use ESP alone or in combination with AH to provide additional authentication. AH protects data from modification but does not provide confidentiality.

SA is the configuration information that specifies the type of security provided to the IPSec flow. The SA is a set of algorithms and keys used to authenticate and encrypt the traffic flow. The AH and ESP use SA to provide traffic protection for the IPSec flow.

NOTE:
Due to performance limitations on the control processor, you cannot enable IPSec on all packets in a communication session.

Topics:

- crypto ipsec transform-set
- crypto ipsec policy
- management crypto-policy
- match
- session-key
- show crypto ipsec transform-set
- show crypto ipsec policy
- transform-set

crypto ipsec transform-set

Create a transform set, or combination of security algorithms and protocols, of cryptos.

C9000 Series

Syntax

`crypto ipsec transform-set` *name* `{ah-authentication {md5|sha1|null} | esp-authentication {md5|sha1|null} | esp-encryption {3des|cbc|des|null}}`

To delete a transform set, use the `no crypto ipsec transform-set` *name* `{ah-authentication {md5|sha1|null} | esp-authentication {md5|sha1|null} | esp-encryption {3des|cbc|des|null}}` command.

Parameters

name — Enter the name for the transform set.

ah-authentication — Enter the keywords `ah-authentication` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.

- md5 — Use Message Digest 5 (MD5) authentication.
- sha1 — Use Secure Hash Algorithm 1 (SHA-1) authentication.
- null — Causes an encryption policy configured for the area to not be inherited on the interface.

esp-authentication — Enter the keywords `esp-authentication` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.

- md5 — Use Message Digest 5 (MD5) authentication.
- sha1 — Use Secure Hash Algorithm 1 (SHA-1) authentication.
- null — Causes an encryption policy configured for the area to not be inherited on the interface.

esp-encryption — Enter the keywords `esp-encryption` then the transform type of operation to apply to traffic. The transform type represents the encryption or authentication applied to traffic.

- 3des — Use 3DES encryption.
- cbc — Use CDC encryption.
- des — Use DES encryption.
- null — Causes an encryption policy configured for the area to not be inherited on the interface.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

Usage Information

- Both sides of the link must specify the same transform set.
- You can create up to 64 transform sets.

Example

```
Dell(conf)#int ten 0/4
Dell(conf-if-te-0/4)#ipv6 address 200:1::/64 eui64
Dell(conf)#int ten 0/6
Dell(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64
```

crypto ipsec policy

Create a crypto policy used by ipsec.

C9000 Series

Syntax

`crypto ipsec policy` *`name seq-num`* `ipsec-manual`

To delete a crypto policy entry, use the `no crypto ipsec policy` *`name seq-num`* `ipsec-manual` command.

Parameters

name	Enter the name for the crypto policy set.
seq-num	Enter the sequence number assigned to the crypto policy entry.

Defaults none

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

Usage Information

This command creates a crypto policy entry and enters the crypto policy configuration mode for configuring the flow parameters.

Example

```
Dell(conf)#crypto ipsec policy West 10 ipsec-manual
Dell(conf-crypto-policy)#
```

management crypto-policy

Apply the crypto policy to management traffic.

C9000 Series

Syntax

`management crypto-policy name`

To remove the management traffic crypto policy, use the `no management crypto-policy name` command.

Parameters

name	Enter the name for the crypto policy..

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

match

Apply a match filter to the crypto policy.

C9000 Series

Syntax

`match seq-num tcp [sourceip address | ipv6 address {mask} {source-port number}] [destination ip address | ipv6 address {mask} {destination-port number}]`

To remove the match filter for the crypto map, use the `no match seq-num tcp [source ip address | ipv6 address {mask} {source-port number}] [destination ip address | ipv6 address {mask} {destination-port number}]` command.

Parameters

seq-num	Enter the match command sequence number.
source*ip-address | ipv6 address*	Enter the keyword `source` then the IPv4 or IPv6 address for the source.
mask	Enter the mask prefix length in /nn format.
source-port number	Enter the source port number.

destination-port number	Enter the destination port number.

Defaults none

Command Modes CONFIG-CRYPTO-POLICY

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

Usage Information

- IPv4 addresses support only -/32 mask types.
- IPv6 addresses support only -/128 mask types.
- Configure match for bi-directional traffic for optimal routing.
- Only TCP is supported.

Example

```
match 0 tcp a::1 /128 0 a::2 /128 23
match 1 tcp a::1 /128 23 a::2 /128 0
match 2 tcp a::1 /128 0 a::2 /128 21
match 3 tcp a::1 /128 21 a::2 /128 0
match 4 tcp 1.1.1.1 /32 0 1.1.1.2 /32 23
match 5 tcp 1.1.1.1 /32 23 1.1.1.2 /32 0
match 6 tcp 1.1.1.1 /32 0 1.1.1.2 /32 21
match 7 tcp 1.1.1.1 /32 21 1.1.1.2 /32 0
```

session-key

Specify the session keys used in the crypto policy entry.

C9000 Series

Syntax `session-key {inbound | outbound} {ah` *`spi hex-key-string`* `| esp` *`spi`* `encrypt` *`hex-key-string`* `auth` *`hex-key-string`*

To delete the session key information from the crypto policy, use the `no session-key {inbound | outbound} {ah | esp}` command.

Parameters

name	Enter the name for the transform set.
inbound	Specify the inbound session key for IPSec.
outbound	Specify the outbound session key for IPSec.
ah	Use the AH protocol when you select the AH transform set in the crypto policy.

esp	Use the ESP protocol when you select the ESP transform set in the crypto policy.
spi	Enter the security parameter index number.
hex-key-string	Enter the session key in hex format (a string of 8, 16, or 20 bytes). For DES algorithms, specify at least 16 bytes per key. For SHA algorithms, specify at least 20 bytes per key.
encrypt	Indicates the ESP encryption transform set key string.
auth	Indicates the ESP authentication transform set key string.

Defaults none

Command Modes CONF-CRYPTO-POLICY

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

Usage Information

- This command is only available in the ipsec-manual model.
- The key information entry is associated with the global method for enabling clear text or encrypted display in the running config.

show crypto ipsec transform-set

Display the transform set configuration.

C9000 Series

Syntax `show crypto ipsec transform-set name`

Parameters

name	Enter the name of the transform set.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell#show crypto ipsec transform-set

Transform-Set Name    : dallas
Transform-Set refCnt  : 0
AH Transform          :
ESP Auth Transform    :
ESP Encry Transform   : 3des
Dell#
```

show crypto ipsec policy

Display the crypto policy configuration.

C9000 Series

Syntax `show crypto ipsec policy`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

Example

```
Dell#show crypto ipsec policy

Policy name           : West
Policy refcount       : 1
Sequence Num          : 10
SA Mode               : IPSEC-MANUAL
Transform-Set Name    : dallas
Peer IP Address       :
Inbound AH SPI        : 0
Inbound ESP Auth SPI  : 0
Inbound ESP Encry SPI : 256
Inbound AH Key        : [0]::
Inbound ESP Auth Key  : [0]::
Inbound ESP Encry Key : [96]::a5b6b42009d47895b420a5b6789509d
4b420a5b6789509d4b420a5b6789509d4b420a5b6789509d4b420a5b6789509d4
Outbound AH SPI       : 0
Outbound ESP Auth SPI : 0
Outbound ESP Encry SPI: 257
Outound AH Key        : [0]::
Outound ESP Auth Key  : [0]::
Outound ESP Encry Key : [96]::a5b6b42009d47895b420a5b6789509d
4b420a5b6789509d4b420a5b6789509d4b420a5b6789509d4b420a5b6789509d4
```

```
  Match sequence Num    : 0
  Protocol type         : tcp
  IP or IPv6            : IPv6
  Source address        : a::1
  Source mask           : /128
  Source port           : 0
  Destination address   : a::2
  Destination mask      : /128
  Destination port      : 23
  source-interface name :
  source-interface num  :


  Match sequence Num    : 1
  Protocol type         : tcp
  IP or IPv6            : IPv6
  Source address        : a::1
  Source mask           : /128
  Source port           : 23
  Destination address   : a::2
  Destination mask      : /128
  Destination port      : 0
  source-interface name :
  source-interface num  :


  Match sequence Num    : 2
  Protocol type         : tcp
  IP or IPv6            : IPv6
  Source address        : a::1
  Source mask           : /128
  Source port           : 0
  Destination address   : a::2
  Destination mask      : /128
  Destination port      : 21
  source-interface name :
  source-interface num  :


  Match sequence Num    : 3
  Protocol type         : tcp
  IP or IPv6            : IPv6
  Source address        : a::1
  Source mask           : /128
  Source port           : 21
  Destination address   : a::2
  Destination mask      : /128
  Destination port      : 0
  source-interface name :
  source-interface num  :

Dell#
```

transform-set

Specify the transform set for crypto policy use.

C9000 Series

Syntax `transform-set` *transform-set-name*

To delete a transform set from the crypto policy, use the `no transform-set` *`transform-set-name`* command.

Parameters

transform-set-name	Enter the name for the crypto policy transform set.

Defaults none

Command Modes CONFIG-CRYPTO-POLICY

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Descrption
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000, S4810, and S4820T.

26

IPv4 Routing

The basic IPv4 commands are supported by Dell Networking operating system on the switch.

Topics:

- arp
- arp backoff-time
- arp learn-enable
- arp retries
- arp timeout
- clear arp-cache
- clear host
- clear ip fib linecard
- clear ip route
- clear ip traffic
- clear tcp statistics
- debug arp
- debug ip dhcp
- debug ip icmp
- debug ip packet
- deny arp (for Extended MAC ACLs)
- icmp6-redirect enable
- ip address
- ip directed-broadcast
- ip domain-list
- ip domain-lookup
- ip domain-name
- ip helper-address hop-count disable
- ip host
- ip max-frag-count
- ip name-server
- ip proxy-arp
- ip route
- ip source-route
- ip unreachables
- ipv4 unicast-host-route
- load-balance
- management route
- show arp
- show arp retries
- show hosts
- show ip cam linecard

- show ip fib linecard
- show ip flow
- show ip interface
- show ip management-route
- show ipv6 management-route
- show ip protocols
- show ip route
- show ip route list
- show ip route summary
- show ip traffic
- show tcp statistics

arp

To associate an IP address with a MAC address in the switch, use address resolution protocol (ARP).

C9000 Series

Syntax

`arp [vrf vrf-name]ip-address mac-address interface`

To remove an ARP address, use the `no arp ip-address` command.

Parameters

vrf *vrf-name*	Enter a VRF name to configure an ARP entry for that VRF. Use the VRF option after the keyword `arp` to configure a static arp on that particular VRF.
ip-address	Enter an IP address in dotted decimal format.
mac-address	Enter a MAC address in nnnn.nnnn.nnnn format.
interface	Enter any of the following keywords and slot/port or number information: • For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id*, stack-unit *unit number*, and port-ID. The *pe-id* range is 0–255; the stack-unit *unit number* range is 0–7; and the port-id range is 0–48. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults Not configured.

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

You cannot use Class D or Class E IP addresses or zero IP address (0.0.0.0) when creating a static ARP. Zero MAC addresses (00:00:00:00:00:00) are also invalid.

Use this command in Configuration Terminal Batch mode to associate an IP address with a MAC address in a dual-homing setup.

NOTE: The parameters vrf, mac-address, and interface are not supported in the batch mode.

Although static ARP entries take precedence over dynamically-learnt ARP entries, a static ARP entry that points to a wrong port is not included in the FIB or ARP entries.

Related Commands

clear arp-cache — clears dynamic ARP entries from the ARP table.

show arp — displays the ARP table.

arp backoff-time

Set the exponential timer for resending unresolved ARPs.

C9000 Series

Syntax

```
arp backoff-time seconds / minutes
```

Parameters

seconds	Enter the number of seconds an ARP entry is black-holed. The range is from 1 to 3600. The default is **30** minutes.
minutes	Enter the number of minutes an ARP entry is balck-holed. The range is from 0 to 35790. The default is **4** hours.

Defaults **30**

Command Mode CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information The `arp backoff` timer is an exponential backoff timer. Over the specified period, the time between ARP requests increases. This behavior reduces the potential for the system to slow down while waiting for a multitude of ARP responses.

Related Commands show arp retries — displays the configured number of ARP retries.

arp learn-enable

Enable ARP learning using gratuitous ARP.

C9000 Series

Syntax `arp learn-enable`

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced.

arp retries

Set the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

C9000 Series

Syntax `arp retries number`

Parameters

number	Enter the number of retries. The range is from 5 to 20. The default is **5**.

Defaults **5**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced.

Usage Information Retries are 20 seconds apart.

Related Commands show arp retries — displays the configured number of ARP retries.

arp timeout

Set the time interval for an ARP entry to remain in the ARP cache.

C9000 Series

Syntax

```
arp timeout minutes
```

Parameters

minutes	Enter the number of minutes. The range is from 0 to 35790. The default is **4 hours (240 minutes)**.

Defaults

240 minutes (4 hours)

Command Modes

- INTERFACE
- INTERFACE PORT EXTENDER (conf-if-pegi-*pe-id*/ stack-unit / port-id)
- INTERFACE (BATCH MODE)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

show interfaces — displays the ARP timeout value for all available interfaces.

clear arp-cache

Clear the dynamic ARP entries from a specific interface or optionally delete (`no-refresh`) ARP entries from the content addressable memory (CAM).

C9000 Series

Syntax

```
clear arp-cache [interface | ip ip-address] [no-refresh]
```

Parameters

interface (OPTIONAL) Enter the following keywords and slot/port or number information:

- For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

ip *ip-address* (OPTIONAL) Enter the keyword `ip` then the IP address of the ARP entry you wish to clear.

no-refresh (OPTIONAL) Enter the keywords `no-refresh` to delete the ARP entry from CAM. Or use this option with *`interface`* or `ip` *`ip-address`* to specify which dynamic ARP entries you want to delete.

NOTE: Transit traffic may not be forwarded during the period when deleted ARP entries are resolved again and reinstalled in CAM. Use this option with extreme caution.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

clear host

Remove one or all dynamically learned host table entries.

C9000 Series

Syntax `clear host name`

Parameters

name	Enter the name of the host to delete. Enter * to delete all host table entries.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

clear ip fib linecard

Clear all FIB entries on a line card (use this command with caution; refer to *Usage Information*.)

C9000 Series

Syntax `clear ip fib linecard slot—id`

Parameters

linecard *slot-id*	Enter the slot ID of a line card. Valid slot IDs are from 0 to 2.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.19.0	Introduced on the S4820T.

Usage Information To clear Layer 3 CAM inconsistencies, use this command.

CAUTION: Executing this command causes traffic disruption.

Related Commands show ip fib linecard — shows FIB entries on a specified stack-unit.

clear ip route

Clear one or all routes in the routing table.

C9000 Series

Syntax `clear ip route {* | ip-address mask}`

Parameters

*****	Enter an asterisk (*) to clear all learned IP routes.
ip-address mask	Enter a specific IP address and mask in dotted decimal format to clear that IP address from the routing table.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

- ip route — assigns an IP route to the switch.
- show ip route — views the routing table
- show ip route summary — views a summary of the routing table.

clear ip traffic

Clear IP traffic statistics on the switch CPUs.

C9000 Series

Syntax

```
clear ip traffic {cp | rp}
```

Parameters

cp	Clear ip traffic statistics on the Control Processor CPU.
rp	Clear ip traffic statistics on the Route Processor CPU.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands show ip traffic — displays IP traffic statistics.

clear tcp statistics

Clear TCP counters.

C9000 Series

Syntax `clear tcp statistics [all | cp | rp]`

Parameters

all	Enter the keyword `all` to clear TCP statistics maintained on all switch processors.
cp	(OPTIONAL) Enter the `cp` to clear TCP statistics only from the Control Processor.
rp	(OPTIONAL) Enter the keyword `rp1` to clear TCP statistics only from the Route Processor.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands show tcp statistics — displays TCP traffic statistics.

debug arp

View information on ARP transactions.

C9000 Series

Syntax `debug arp [interface] [count value]`

To stop debugging ARP transactions, use the `no debug arp` command.

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id*information. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
count *value*	(OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Added the `count` option.

Usage Information To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

debug ip dhcp

Enable debug information for dynamic host configuration protocol (DHCP) relay transactions and display the information on the console.

C9000 Series

Syntax `debug ip dhcp`

To disable debug, use the `no debug ip dhcp` command.

Defaults Debug disabled

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.10	Introduced on the E-Series.

Example

```
Dell#debug ip dhcp
00:12:21 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface
```

```
113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 0, hwaddr = 00:60:CF:20:7B:8C,
teaddr = 0.0.0.0
00:12:21 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C
to 14.4.4.2
00:12:26 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface
113.3.3.17 BOOTP
Request, hops = 0, XID = 0xbf05140f, secs = 5, hwaddr = 00:60:CF:20:7B:8C,
teaddr = 0.0.0.0
00:12:26 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C
to 14.4.4.2
00:12:40 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface
113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C,
teaddr = 0.0.0.0
00:12:40 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C
to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface
14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, teaddr =
113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to
113.3.3.254
00:12:42 : %RELAY-I-PACKET: BOOTP REQUEST (Unicast) received at interface
113.3.3.17 BOOTP
Request, hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C,
teaddr = 0.0.0.0
00:12:42 : %RELAY-I-BOOTREQUEST: Forwarded BOOTREQUEST for 00:60:CF:20:7B:8C
to 14.4.4.2
00:12:42 : %RELAY-I-PACKET: BOOTP REPLY (Unicast) received at interface
14.4.4.1 BOOTP Reply,
hops = 0, XID = 0xda4f9503, secs = 0, hwaddr = 00:60:CF:20:7B:8C, teaddr =
113.3.3.17
00:12:42 : %RELAY-I-BOOTREPLY: Forwarded BOOTREPLY for 00:60:CF:20:7B:8C to
113.3.3.254
Dell#
```

Related Commands

- ip helper-address – specifies the destination broadcast or host address for the DHCP server request.
- ip helper-address hop-count disable – disables the hop-count increment for the DHCP relay agent.

debug ip icmp

View information on the internal control message protocol (ICMP).

C9000 Series

Syntax

`debug ip icmp [interface] [count value]`

To disable debugging, use the `no debug ip icmp` command.

Parameters

interface (OPTIONAL) Enter the following keywords and slot/port or number information:

- For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

- For a Tunnel interface, enter the keywords `tunnel` then a number. The range is from 1 to 16383.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id*/stack-unit/port information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

count *value* (OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534. The default is **Infinity**.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Added the `count` option.

Example

```
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
ICMP: echo request rcvd from src 40.40.40.40
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: src 40.40.40.40, dst 40.40.40.40, echo reply
ICMP: echo request sent to dst 40.40.40.40
```

Usage Information To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

debug ip packet

View a log of IP packets sent and received.

C9000 Series

Syntax

`debug ip packet [access-group` *`name`*`] [count` *`value`*`] [`*`interface`*`]`

To disable debugging, use the `no debug ip packet [access-group` *`name`*`] [count` *`value`*`] [`*`interface`*`]` command.

Parameters

access-group *name*	Enter the keyword `access-group` then the access list name (maximum 16 characters) to limit the debug output based on the defined rules in the ACL.
count *value*	(OPTIONAL) Enter the keyword `count` then the count value. The range is from 1 to 65534. The default is `Infinity`.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For the Management interface, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0. • For a Port Channel interface, enter the keywords `port-channel` then a number. For the C-Series and S-Series, the range is from 1 to 4096. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Added the `access-group` option.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Added the `count` option.

Usage Information

The following describes the `debug ip packet` command in the following example.

Field	Description
s=	Lists the source address of the packet and the name of the interface (in parentheses) that received the packet.
d=	Lists the destination address of the packet and the name of the interface (in parentheses) through which the packet is being sent out on the network.
len	Displays the packet's length.
sending, rcvd, fragment, sending broad/multicast proto, unroutable	The last part of each line lists the status of the packet.
TCP src=	Displays the source and destination ports, the sequence number, the acknowledgement number, and the window size of the packets in that TCP packets.
UDP src=	Displays the source and destination ports for the UDP packets.
ICMP type=	Displays the ICMP type and code.
IP Fragment	States that it is a fragment and displays the unique number identifying the fragment (Ident) and the offset (in 8-byte units) of this fragment (fragment offset) from the beginning of the original datagram.

Example

```
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 54, sending
    TCP src=23, dst=40869, seq=2112994894, ack=606901739, win=8191 ACK PUSH
IP: s=10.1.2.206 (Ma 0/0), d=10.1.2.62, len 40, rcvd
    TCP src=0, dst=0, seq=0, ack=0, win=0
IP: s=10.1.2.62 (local), d=10.1.2.206 (Ma 0/0), len 226, sending
    TCP src=23, dst=40869, seq=2112994896, ack=606901739, win=8192 ACK PUSH
IP: s=10.1.2.216 (Ma 0/0), d=10.1.2.255, len 78, rcvd
    UDP src=0, dst=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment
    IP Fragment, Ident = 4741, fragment offset = 0
    ICMP type=0, code=0
IP: s=10.1.2.62 (local), d=10.1.2.3 (Ma 0/0), len 1500, sending fragment
    IP Fragment, Ident = 4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (Te 2/11), len 64, sending broad/
multicast
proto=89
IP: s=40.40.40.40 (local), d=224.0.0.6 (Te 2/11), len 28, sending broad/
multicast
proto=2
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
```

```
   ICMP type=8, code=0
IP: s=0.0.0.0, d=30.30.30.30, len 100, unroutable
   ICMP type=8, code=0
```

Usage Information

To stop packets from flooding the user terminal when debugging is turned on, use the `count` option.

The `access-group` option supports only the equal to (`eq`) operator in TCP ACL rules. Port operators not equal to (`neq`), greater than (`gt`), less than (`lt`), or `range` are not supported in access-group option (refer to the following example). ARP packets (`arp`) and Ether-type (`ether-type`) are also not supported in the `access-group` option. The entire rule is skipped to compose the filter.

The `access-group` option pertains to:

- IP protocol number: from 0 to 255
- Internet control message protocol (`icmp`) but not the ICMP message type (from 0 to 255)
- Any internet protocol (`ip`)
- Transmission Control Protocol (`tcp`) but not on the `rst`, `syn`, or `urg` bits
- User Datagram Protocol (`udp`)

If an ambiguous access control list rules, the `debug ip packet access-control` command is disabled. A message appears identifying the error (refer to the following Example).

Example (Error Messages)

```
Dell#debug ip packet access-group test
%Error: port operator GT not supported in access-list debug
%Error: port operator LT not supported in access-list debug
%Error: port operator RANGE not supported in access-list debug
%Error: port operator NEQ not supported in access-list debug

Dell#00:10:45: %RPM0-P:CP
%IPMGR-3-DEBUG_IP_PACKET_ACL_AMBIGUOUS_EXP: Ambiguous rules not
supported in access-list debug, access-list debugging is turned off
Dell#
```

deny arp (for Extended MAC ACLs)

Configure an egress filter that drops ARP packets on egress ACL supported line cards. (For more information, refer to your line card documentation).

C9000 Series

Syntax

`deny arp {`*`destination-mac-address mac-address-mask`* `| any} vlan` *`vlan-id`* `{`*`ip-address`* `| any | opcode code-`*`number`*`} [count [byte]] [order] [log [interval`* *`minutes`*`] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq` *`sequence-number`* command if you know the filter's sequence number.
- Use the `no deny arp {`*`destination-mac-address mac-address-mask`* `| any} vlan` *`vlan-id`* `{`*`ip-address`* `| any | opcode`* *`code-number`*`}` command.

Parameters

log (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Command Modes CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based `enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

icmp6-redirect enable

Enable ICMP and ICMP6 redirects.

Syntax `icmp6-redirect enable`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
Legacy command	Legacy command

Usage Information

Use this command to notify hosts on the same network that a better route is available for a specific destination.

The `icmp6-redirect enable` command is applicable for both IP and IPv6 routes.

ip address

Assign a primary and secondary IP address to the interface.

C9000 Series

Syntax

`ip address {`*`ip-address mask`* `[secondary] | dhcp}`

To delete an IP address from an interface, use the `no ip address [`*`ip-address`*`]` command.

Parameters

ip-address	Enter an IP address in dotted decimal format.
mask	Enter the mask of the IP address in slash prefix format (for example, /24).
secondary	(OPTIONAL) Enter the keyword `secondary` to designate the IP address as the secondary address.
dhcp	Enter the keyword `dhcp` to configure an interface to receive its IP address from the configured DHCP server.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information You must be in INTERFACE mode before you add an IP address to an interface. Assign an IP address to an interface prior to entering ROUTER OSPF mode.

ip directed-broadcast

Enable the interface to receive directed broadcast packets.

C9000 Series

Syntax `ip directed-broadcast`

To disable the interface from receiving directed broadcast packets, use the `no ip directed-broadcast` command.

Defaults Disabled (that is, the interface does not receive directed broadcast packets)

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

ip domain-list

Configure ip domain names to complete unqualified host names.

C9000 Series

Syntax `ip domain-list` *`name`*

To remove the name, use the `no ip domain-list` *`name`* command.

Parameters

name	Enter an ip domain name to complete unqualified names (that is, incomplete domain names that cannot be resolved).

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information To configure a list of possible domain names, configure the `ip domain-list` command up to six times.

If you configure both the `ip domain-name` and `ip domain-list` commands, the software tries to resolve the name using the `ip domain-name` command. If the name is not resolved, the software goes through the list of names configured with the `ip domain-list` command to find a match.

To enable dynamic resolution of hosts, use the following steps:

- specify a domain name server with the `ip name-server` command
- enable DNS with the `ip domain-lookup` command

To view current bindings, use the `show hosts` command. To view a DNS-related configuration, use the `show running-config resolve` command.

Related Commands ip domain-name — specifies a DNS server.

ip domain-lookup

Enable dynamic host-name to address resolution (that is, DNS).

C9000 Series

Syntax `ip domain-lookup`

To disable DNS lookup, use the `no ip domain-lookup` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information To fully enable DNS, also specify one or more domain name servers with the `ip name-server` command.

The system does not support sending DNS queries over a VLAN. DNS queries are sent out on all other interfaces, including the Management port.

To view current bindings, use the `show hosts` command.

Related Commands

- ip name-server — specifies a DNS server
- show hosts — Views the current bindings.

ip domain-name

Configure one domain name for the switch.

C9000 Series

Syntax `ip domain-name` *name*

To remove the domain name, use the `no ip domain-name` command.

Parameters

name	Enter one domain name to complete unqualified names (that is, incomplete domain names that cannot be resolved).

Defaults Not configured.

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

You can only configure one domain name with the `ip domain-name` command. To configure more than one domain name, configure the `ip domain-list` command up to six times.

To enable dynamic resolution of hosts, use the following steps:

- specify a domain name server with the `ip name-server` command
- enable DNS with the `ip domain-lookup` command

To view current bindings, use the `show hosts` command.

Related Commands

ip domain-list — configures additional names.

ip helper-address hop-count disable

Disable the hop-count increment for the DHCP relay agent.

C9000 Series

Syntax

```
ip helper-address hop-count disable
```

To re-enable the hop-count increment, use the `no ip helper-address hop-count disable` command.

Defaults

Enabled; the hops field in the DHCP message header is incremental by default.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced for the E-Series.

Usage Information

This command disables the hop field increments when boot requests are relayed to a DHCP server through the system. If the incoming boot request already has a non-zero hops field, the message is relayed with the same value for hops. However, the message is discarded if the hops field exceeds 16, to comply with the relay agent behavior specified in RFC 1542.

Related Commands

- ip helper-address — specifies the destination broadcast or host address for DHCP server requests.
- show running-config — displays the current configuration and changes from the default values.

ip host

Assign a name and IP address for the host-to-IP address mapping table.

C9000 Series

Syntax

`ip host name` *`ip-address`*

To remove an IP host, use the `no ip host name [`*`ip-address`*`]` command.

Parameters

name	Enter a text string to associate with one IP address.
ip address	Enter an IP address, in dotted decimal format, to be mapped to the name.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced for the E-Series.

ip max-frag-count

Set the maximum number of fragments allowed in one packet for packet re-assembly.

C9000 Series

Syntax

`ip max-frag-count` *count*

To place no limit on the number of fragments allowed, use the `no ip max-frag-count` command.

Parameters

count	Enter a number for the number of fragments allowed for re-assembly. The range is from 2 to 256.

Defaults

No limit is set on number of fragments allowed.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced for the E-Series.

Usage Information To avoid denial of service (DOS) attacks, keep the number of fragments allowed for re-assembly low.

ip name-server

Enter up to six IPv4 addresses of name servers. The order you enter the addresses determines the order of their use.

C9000 Series

Syntax `ip name-server ipv4-address [ipv4-address2...ipv4-address6]`

To remove a name server, use the `no ip name-server ip-address` command.

Parameters

ipv4-address	Enter the IPv4 address, in dotted decimal format, of the name server to be used.
ipv4-address2... ipv4-address6	(OPTIONAL) Enter up five more IPv4 addresses, in dotted decimal format, of name servers to be used. Separate the addresses with a space.

Defaults No name servers are configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The system does not support sending DNS queries over a VLAN. DNS queries are sent out on all other interfaces, including the Management port.

You can separately configure both IPv4 and IPv6 domain name servers.

Related Commands ipv6 name-server — configures an IPv6 name server.

ip proxy-arp

Enable proxy ARP on an interface.

C9000 Series

Syntax

`ip proxy-arp`

To disable proxy ARP, use the `no ip proxy-arp` command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

show ip interface — displays the interface routing status and configuration.

ip route

Assign a static route to the switch.

C9000 Series

Syntax

`ip route {`*`destination mask {ip-address`*` | interface [`*`slot/port`*`] | [tunnel `*`tunnel-id`*`] [`*`distance`*`] [name `*`description`*`] [permanent] | tag `*`tag-value`*`}}[vrf `*`vrf-name`*` ]`

To delete a specific static route, use the `no ip route `*`destination mask`* command.

To delete all routes matching a certain route, use the `no ip route destination mask` command.

Parameters

destination	Enter the IP address in dotted decimal format of the destination device.
mask	Enter the mask in the slash prefix format (/x) of the destination IP address.
ip-address	Enter the IP address of the forwarding router in dotted decimal format.
interface *interface*	Enter one of the following keywords and slot/port or number information: • For a null interface, enter the keyword `null` then the slot/port information. The Null interface number is 0. • For a Management Ethernet interface, enter the keyword `managementethernet` then the slot/port information. • For a Loopback interface, enter the keyword `loopback` then the slot/port information. The range is from 0 to 16383. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383. • For a VLAN interface, enter the keyword `vlan` then the slot/port information. The range is from 1 to 4094. • For a port extender (PE) Gigabit Ethernet interface, enter the keyword peGigE then the *pe-id / stack-unit / port-id* information. The *pe-id* range is 0–255; the stack-unit *number* range is 0– 7; and the *port-id* range is 1–48. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE. If you configure a static IPv6 route using an egress interface and enter the ping command to reach the destination IPv6 address, the ping operation may not work. Configure the IPv6 route using a next-hop IPv6 address in order for the ping command to detect the destination address.
interface *ip-address*	Enter the keyword `interface` then the IP address.
name *description*	(OPTIONAL) Enter the keyword `name` and the description for the IPv4 static route configuration.
distance	(OPTIONAL) Enter the value of the distance metric assigned to the route. The range is from 1 to 255.
permanent	(OPTIONAL) Enter the keyword `permanent` to specify that the route must not be removed even if the interface assigned to that route goes down. The route must be currently active to be installed in the routing table. If you disable the interface, the route is removed from the routing table.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` then a number to assign to the route. The range is from 1 to 4294967295.
vrf *vrf-name*	Enter the keyword `vrf` followed by the name of the VRF. Use this VRF option after the next hop to specify which VRF the next hop belongs to. This setting is used in route leaking cases. Refer to the Route Leaking VRFs section in the Virtual Routing and Forwarding (VRF) chapter of the Configuration guide.

weight *weight-value*	Enter the keyword `weight` followed by a weight value. The range is from 0 to 255. **NOTE: Weight for a static route can be added only for the destination address and not for the route pointing to destination a interface.**

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.14(1.2)	Added the keyword `name` for static routes.
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Included the `weighted` parameter to support weighted ECMP feature.
9.4.(0.0)	Added support for VRF.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.2.(0.0)	Added support for tunnel interface type.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

Usage Information Using the following example of a static route: ip route 33.33.33.0 /24 tengigabitethernet 1/1 172.31.5.43

- The software installs a next hop that is not on the directly connected subnet but which recursively resolves to a next hop on the interface's configured subnet. In the example, if tengig 1/1 has an ip address on subnet 2.2.2.0 and if 172.31.5.43 recursively resolves to 2.2.2.0, Dell Networking OS installs the static route.
- When the interface goes down, Dell Networking OS withdraws the route.
- When the interface comes up, Dell Networking OS re-installs the route.

- When recursive resolution is “broken,” Dell Networking OS withdraws the route.
- When recursive resolution is satisfied, Dell Networking OS re-installs the route.

You can specify a weight for an IPv4 or IPv6 static route. If the weight value of a path is 0, then that path is not used for forwarding when weighted ECMP is in effect. Also, if a path corresponding to a static route (destination) has a non-zero weight assigned to it and other paths do not have any weight configured, then regular ECMP is used for forwarding.

You can specify the weight value only to destination address and not on the egress port.

A route is considered for weighted ECMP calculations only if each path corresponding to that route is configured with a weight.

You cannot use the VRF attribute of this command to configure routes in a management VRF. When a specific VRF is deleted, all the configured static routes corresponding to that VRF are automatically removed.

Example

```
Dell(conf)#ip route 1.1.1.0/24 4.4.4.2 weight 100
Dell(conf)#ip route 1.1.1.0/24 6.6.6.2 weight 200
Dell(conf)#do show running-config | grep route ip route 1.1.1.0/24 4.4.4.2
weight 100 ip route 1.1.1.0/24 6.6.6.2 weight 200
Dell(conf)#ip route  vrf test 1.1.1.0/24 4.4.4.2 weight 100
Dell(conf)#ip route vrf test  1.1.1.0/24 6.6.6.2 weight 200
Dell(conf)#
Dell(conf)#do show running-config | grep route ip route vrf test  1.1.1.0/24
4.4.4.2 weight 100 ip route vrf test  1.1.1.0/24 6.6.6.2 weight 200
```

Related Commands show ip route — views the switch routing table.

ip source-route

Enable the system to forward IP packets with source route information in the header.

C9000 Series

Syntax `ip source-route`

To drop packets with source route information, use the `no ip route-source` command.

Defaults Enabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ip unreachables

Enable the generation of internet control message protocol (ICMP) unreachable messages.

C9000 Series

Syntax

```
ip unreachables
```

To disable the generation of ICMP messages, use the `no ip unreachables` command.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ipv4 unicast-host-route

Enable the storage of IPv4 route prefixes in the L3 host table.

C9000 Series

Syntax `[no] ipv4 unicast-host-route`

Defaults Disabled; by default, all IPv4 route prefixes are stored installed only in the Longest Prefix Match (LPM) table.

Command Modes CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.3(0.1)	Introduced on the S6000.

Usage Information Route prefixes stored in the L3 host table are managed using ECMP next-hop forwarding.

A warning message is displayed after you enter the command stating that this setting takes effect for existing routes only when IPv4 route prefixes are cleared from the LPM routing table (RTM). To enable storage of IPv4 route prefixes in the LPM table, disable this setting by entering the `no ipv4 unicast-host-route` command.

Example

```
Dell(conf)#ipv4 unicast-host-route
Warning: Command will take effect for existing routes only when IPv4
route prefixes are cleared from RTM
Dell(conf)#no ipv4 unicast-host-route
```

load-balance

By default, the system uses an IP 4-tuple (IP SA, IP DA, Source Port, and Destination Port) to distribute IP traffic over members of a Port Channel as well as equal-cost paths. To designate another method to balance traffic over Port Channel members, use the `load-balance` command.

C9000 Series

Syntax `load-balance {ip-selection [dest-ip | source-ip]} | {mac [dest-mac | source-dest-mac | source-mac]} | {tcp-udp | ingress-port [enable]}`

To return to the default setting (IP 4-tuple), use the `no load-balance {ip-selection [dest-ip | source-ip]} | {mac [dest-mac | source-dest-mac | source-mac]} | {tcp-udp | ingress-port [enable]}`command.

Parameters

ip-selection {dest-ip | source-ip} Enter the keywords to distribute IP traffic based on the following criteria:

- `dest-ip` — Uses destination IP address and destination port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.
- `source-ip` — Uses source IP address and source port fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.

mac {dest-mac | source-dest-mac | source-mac}

Enter the keywords to distribute MAC traffic based on the following criteria:

- `dest-mac` — Uses the destination MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.
- `source-dest-mac` — Uses the destination and source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.
- `source-mac` — Uses the source MAC address, VLAN, Ethertype, source module ID and source port ID fields to hash. The hashing mechanism returns a 3-bit index indicating which port the packet should be forwarded.

tcp-udp enable

Enter the keywords to distribute traffic based on the following:

- `enable` — Takes the TCP/UDP source and destination ports into consideration when doing hash computations. This option is enabled by default.

ingress-port enable

Enter the keywords to distribute traffic based on the following:

- `enable` — Takes the source port into consideration when doing hash computations. This option is disabled by default.

Defaults

IP 4-tuple (IP SA, IP DA, Source Port, Destination Port)

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Added the `ingress-port` parameter for the S4810.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

By default, the system distributes incoming traffic based on a hash algorithm using the following criteria:

- IP source address
- IP destination address

- TCP/UDP source port
- TCP/UDP destination port

Related Commands hash-algorithm ecmp — changes the hash algorithm across an ECMP.

management route

Configure a static route that points to the Management interface or a forwarding router.

C9000 Series

Syntax

`management route {{ip-address mask | {ipv6-address prefix-length}} {forwarding-router-address | managementethernet | fortyGigE | vlan | gigabitethernet | tengigabitethernet}}`

To remove a static route, use the `no management route{{ip-address mask | {ipv6-address prefix-length}}{forwarding-router-address | managementethernet | fortyGigE | vlan | gigabitethernet | tengigabitethernet}}` command.

Parameters

ip-address mask	Enter an IP address (dotted decimal format) and mask (/prefix format) of the destination subnet.
ipv6-address prefix-length	Enter an IPv6 address (x:x:x:x::x format) and mask (/prefix format) of the destination subnet. Enter the IPv6 address in the x:x:x:x::x format followed by the prefix length in the /x format. The range is from /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
forwarding-router-address	Enter an IP address (dotted decimal format) or an IPv6 address (x:x:x:x::x format) of a forwarding router.
managementethernet	Enter the keyword `managementethernet` for the Management interface on the Primary RPM.
fortyGigE	Enter the keyword `fortyGigE` to specify a forty Gigbit Ethernet interface.
vlan	Enter the keyword `vlan` to specify a vlan interface.
gigbitethernet	Enter the keyword `gigabitethernet` to specify a one Gigabit Ethernet interface.
tengigabitethernet	Enter the keyword tengigabitethernet to specify a ten Gigabit Ethernete interface.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Added support for forty gigabit, vlan, and tengigabit ethernet interfaces. Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000 and added support for IPv6.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

Usage Information When a static route (or a protocol route) overlaps with Management static route, the static route (or a protocol route) is preferred over the Management Static route. Also, Management static routes and the Management Connected prefix are not reflected in the hardware routing tables. Separate routing tables are maintained for IPv4 and IPv6 management routes. This command manages both tables.

Related Commands interface ManagementEthernet — configures the Management port on the system (either the Primary or Standby RPM).

speed (Management interface) — sets the speed for the Management interface.

show arp

Display the ARP table entries learned on a switch CPU.

C9000 Series

Syntax

```
show arp [cpu [cp | rp]] [interface interface | ip ip-address [mask] |
macaddress mac-address mask] [static | dynamic] [summary]
```

Parameters

cpu cp	(OPTIONAL) Enter the keywords `cpu cp` to display the ARP entries learned on the Control Processor.
cpu rp	(OPTIONAL) Enter the keyword `cpu rp` to display the ARP entries learned on the Route Processor.
interface *interface*	To specify an interface, enter one of the following interface types and slot/port or number information: • For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383. • For a Port Channel interface, enter the keyword `port-channel` then a number. The range is from 1 to 4096.

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel`.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id/* stack-unit *unit number* /port-ID information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

linecard *slot-id*
(OPTIONAL) Enter the `interface port-type slot/port` parameters to display the ARP entries learned on a Z9500 port. The range of slot IDs is from 0 to 2.

ip *ip-address mask*
(OPTIONAL) Enter the keyword `ip` with an IP address in the dotted decimal format to display the ARP entries learned with this IP address. Enter the optional IP address mask in the slash prefix format (`/ x`).

macaddress *mac-address mask*
(OPTIONAL) Enter the keyword `macaddress` with a MAC address in nn:nn:nn:nn:nn:nn format to display the ARP entries learned with this MAC address. Enter the optional MAC address mask in nn:nn:nn:nn:nn format also.

static
(OPTIONAL) Enter the keyword `static` to display manually-entered ARP entries.

dynamic
(OPTIONAL) Enter the keyword `dynamic` to display dynamically-learned ARP entries.

summary
(OPTIONAL) Enter the keyword `summary` to view a summary of ARP entries.

Default
Display only the ARP entries learned on the Control Processor.

Command Modes
EXEC Privilege

Command History
This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added support for 4094 VLANs on the E-Series ExaScale (the prior limit was 2094).
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.8.1.0	Augmented to display local ARP entries learned from private VLANs (PVLANs).

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

Use the `show arp` command to display the ARP entries learned on the Control Processor and Route Processor.

The following example shows two VLANs that are associated with a private VLAN (PVLAN) (refer to Private VLAN (PVLAN)).

The following describes the `show arp` command shown in the following example.

Field	Description
Protocol	Displays the protocol type.
Address	Displays the IP address of the ARP entry.
Age(min)	Displays the age (in minutes) of the ARP entry.
Hardware Address	Displays the MAC address associated with the ARP entry.
Interface	Displays the first two letters of the interfaces type and the slot/port associated with the ARP entry.
VLAN	Displays the VLAN ID, if any, associated with the ARP entry.
CPU	Lists which CPU the entries are stored on.

Example

```
Dell>show arp

Protocol  Address  Age(min) Hardware Address Interface VLAN CPU
-------------------------------------------------------------
Internet  192.2.1.254 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.253 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.252 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.251 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.250 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.251 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.250 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.249 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.248 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.247 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.246 1  00:00:c0:02:01:02  Te 0/13  -    CP
Internet  192.2.1.245 1  00:00:c0:02:01:02  Te 0/13  -    CP
```

Example (Private VLAN)

NOTE: In this example, Line 1 shows community VLAN 200 (in primary VLAN 10) in a PVLAN. Line 2 shows primary VLAN 10.

```
Dell#show arp
Protocol Address  Age(min) Hardware Address  Interface VLAN  CPU
-------------------------------------------------------------
Internet 5.5.5.1       -  00:01:e8:43:96:5e  -      Vl 10 pv 200 CP
Internet 5.5.5.10      -  00:01:e8:44:99:55  -      Vl 10        CP
Internet 10.1.2.4      1  00:01:e8:d5:9e:e2  Ma 0/0 -            CP
Internet 10.10.10.4    1  00:01:e8:d5:9e:e2  Ma 0/0 -            CP
Internet 10.16.127.53  1  00:01:e8:d5:9e:e2  Ma 0/0 -            CP
Internet 10.16.134.254 20 00:01:e8:d5:9e:e2  Ma 0/0 -            CP
Internet 133.33.33.4   1  00:01:e8:d5:9e:e2  Ma 0/0 -            CP
```

Usage Information

The following describes the `show arp summary` command shown in the following example.

Field	Description
Total Entries	Lists the total number of ARP entries in the ARP table.
Static Entries	Lists the total number of configured or static ARP entries.
Dynamic Entries	Lists the total number of learned or dynamic ARP entries.
CPU	Lists which CPU the entries are stored on.

Example (Summary)

```
#show arp summary

TotalEntries Static Entries Dynamic Entries CPU
-----------------------------------------------
83             0               83           CP
Dell
```

Related Commands

- ip local-proxy-arp — enables/disables Layer 3 communication in secondary VLANs.
- switchport mode private-vlan — sets PVLAN mode of the selected port.

show arp retries

Display the configured number of ARP retries.

C9000 Series

Syntax

```
show arp retries
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Introduced.

Related Commands

arp retries — sets the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

show hosts

View the host table and DNS configuration.

C9000 Series

Syntax

```
show hosts
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Added support for IPv6 addresses.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show hosts` command in the following example.

Field	Description
Default domain...	Displays the domain name (if configured).
Name/address lookup...	States if DNS is enabled on the system. • If DNS is enabled, the Name/Address lookup is domain service. • If DNS is not enabled, the Name/Address lookup is static mapping
Name servers are...	Lists the name servers, if configured.
Host	Displays the host name assigned to the IP address.
Flags	Classifies the entry as one of the following: • perm — the entry was manually configured and will not time out • temp — the entry was learned and will time out after 72 hours of inactivity. Also included in the flag is an indication of the validity of the route:

Field	Description
	• ok — the entry is valid. • ex — the entry expired. • ?? — the entry is suspect.
TTL	Displays the amount of time until the entry ages out of the cache. For dynamically learned entries only.
Type	Displays IP as the type of entry.
Address	Displays the IP addresses assigned to the host.

Example

```
Dell#show hosts
Default domain is not set
Name/address lookup uses static mappings
Name servers are not set
Host     Flags     TTL   Type   Address
-------- -----     ----  ----   -------
ks       (perm, OK) -     IP     2.2.2.2
4200-1   (perm, OK) -     IP     192.68.69.2
1230-3   (perm, OK) -     IP     192.68.99.2
ZZr      (perm, OK) -     IP     192.71.18.2
Z10-3    (perm, OK) -     IP     192.71.23.1
Dell#
```

Related Commands

traceroute — views the DNS resolution.

ip host — configures a host.

show ip cam linecard

View CAM entries for a port pipe on a line card..

C9000 Series

Syntax

```
show ip cam linecard number port-set pipe-number [ip-address mask [longer-prefixes] | index index-number | summary | vrf vrf instance]
```

Parameters

number	Enter the number of the line card.
pipe-number	Enter the number of the line card's port-pipe. The range is from 0 to 1.
ip-address mask [longer-prefix]	(OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only. Enter the keyword `longer-prefixes` to view routes with a common prefix.
index *index-number*	(OPTIONAL) Enter the keyword `index` then the CAM index number. The range depends on CAM size.
summary	(OPTIONAL) Enter the keyword `summary` to view a table listing route prefixes and the total number of routes that can be entered into the CAM.
vrf instance	(OPTIONAL) E-Series Only: Enter the keyword `vrf` then the VRF instance name to show CAM information as it applies to that VRF instance.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.1.1.2	Introduced on the E-Series ExaScale E600i.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip cam` command shown in the following example.

Field	Description
Index	Displays the CAM index number of the entry.
Destination	Displays the destination route of the index.
EC	Displays the number of equal cost multipaths (ECMP) available for the default route for non-Jumbo line cards. For Jumbo line cards, displays 0,1 when ECMP is more than eight.
CG	Displays 0.
V	Displays a 1 if the entry is valid and a 0 if the entry is for a line card with Catalog number beginning with LC-EF.
C	Displays the CPU bit. 1 indicates that a packet hitting this entry is forwarded to the CP or RP2, depending on Egress port.
Next-Hop	Displays the next hop IP address of the entry.
Vld	Displays the VLAN ID. If the entry is 0, the entry is not part of a VLAN.
Mac Addr	Displays the next-hop router's MAC address.
Port	Displays the egress interface. Use the second half of the entry to determine the interface. For example, in the entry 17cl CP, the CP is the pertinent portion. • CP = control processor • RP2 = route processor 2 • Gi = Gigabit Ethernet interface • So = SONET interface • Te = 10-Gigabit Ethernet interface

Example

```
Dell#show ip cam linecard 0 port-set 0
Destination EC C VId Mac-Addr Port
------------------------------------------------------------------
1.1.32.140/32 0 0 200 00:00:00:00:1f:8a PeGigE <PE-ID>/<Slot>/<Port>
```

show ip fib linecard

View all forwarding information base (FIB) entries.

C9000 Series

Syntax `show ip fib linecard linecard id {vrf <vrf-id>/<A.B.C.D>/summary}`

Parameters

linecard	Displays the fib entries for the mentioned linecard id.
vrf	Displays the fib entries for the mentioned *vrf-id*. Otherwise, *vrf* displays the default *vrf* entries.
A.B.C.D.	Displays the fib entry for the mentioned prefix.
summary	Displays the fib summary.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell>show ip fib linecard 2
Destination           Gateway                         First-Hop      Mac-
Addr           Port       VId    EC
------------------------------------------------------------------
------------------- ----------------- ------------
1.1.32.140/32 via 1.1.32.140, PeGigE PE-ID/Slot/Port  1.1.32.140
00:00:00:00:1f:8a  PeGigE PE-ID/Slot/Port 200  0
```

show ip flow

Show how a Layer 3 packet is forwarded when it arrives at a particular interface.

C9000 Series

Syntax

```
show ip flow interface interface {source-ip address destination-ip address}
{protocol number [tcp | udp]} {src-port number destination-port number}
```

Parameters

interface *interface*	Enter the keyword *interface* then one of the following interface keywords. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
source-ip *address*	Enter the keywords `source-ip` then the IP source address in IP address format.
destination-ip *address*	Enter the keywords `destination-ip` then the IP destination address in IP address format.
protocol *number* [tcp | udp]	Enter the keyword `protocol` then one of the protocol type keywords: `tcp`, `udp`, or `protocol number` The protocol number range is from 0 to 255. .
src-port *number*	Enter the keywords *src-port* then the source port number.
destination-port *number*	Enter the keywords `destination-port` then the destination port number.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.0	Introduced on the E-Series.

Usage Information

This command provides egress port information for a given IP flow. This information is useful in identifying which interface the packet follows in the case of Port-channel and Equal Cost Multi Paths. Use this command for routed packed only. For switched packets, use the `show port-channel-flow` command.

The `show ip flow` command does not compute the egress port information when `load-balance mac hashing` is also configured due to insufficient information (the egress MAC is not available).

S-Series produces the following error message: `%Error: Unable to read IP route table.`

Example

```
Dell#show ip flow interface Te 1/8 189.1.1.1 63.0.0.1 protocol tcp source-port
7898 destination-port 8

flow: 189.1.1.1 63.0.0.1 protocol 6 7868 8976
Ingress interface:Te 1/20
Egress interface:Te 1/14 to 1.7.1.2[CAM hit 103710] unfragmented packet
                 Te 1/10 to 1.2.1.2[CAM hit 103710] fragmented packet
```

show ip interface

View IP-related information on all interfaces.

C9000 Series

Syntax `show ip interface [interface | brief] [linecard slot-id] [configured]`

Parameters

interface (OPTIONAL) Enter the following keywords and slot/port or number information:

- For a Loopback interface, enter the keyword `Loopback` then a number from 0 to 16383.
- For the Management interface, enter the keyword `ManagementEthernet` then zero (0).
- For the Null interface, enter the keyword `null` then zero (0).
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number. The range is from 1 to 16383.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

linecard *slot-id* Enter the `linecard slot-id` parameters to specify the switch ports on a line card. The range of slot IDs is from 0 to 2.

brief (OPTIONAL) Enter the keyword `brief` to view a brief summary of the interfaces and whether an IP address is assigned.

configured	(OPTIONAL) Enter the keyword `configured` to display the physical interfaces with non-default configurations only.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Updated the command output to include the unicast reverse path forwarding (uRPF) status.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.1.1.2	Supported on the E-Series ExaScale E600i.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip interface` command shown in the following example.

Lines	Description
TenGigabitEthernet 0/0...	Displays the interface's type, slot/port, and physical and line protocol status.
Internet address...	States whether an IP address is assigned to the interface. If an IP address is assigned, that address is displayed.
IP MTU is...	Displays IP MTU value.
Inbound access...	Displays the name of the configured incoming access list. If none is configured, the phrase "not set" is displayed.
Proxy ARP...	States whether proxy ARP is enabled on the interface.
Split horizon...	States whether split horizon for RIP is enabled on the interface.
Poison Reverse...	States whether poison for RIP is enabled on the interface.
ICMP redirects...	States if ICMP redirects are sent.
ICMP unreachables...	States if ICMP unreachable messages are sent.

Example

```
Dell# show ip interface tengigabitethernet 2
TenGigabitEthernet 2/0 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent
IP unicast RPF check is not supported

TenGigabitEthernet 2/1 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent
IP unicast RPF check is not supported

TenGigabitEthernet 2/2 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent
IP unicast RPF check is not supported

TenGigabitEthernet 2/3 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent
IP unicast RPF check is not supported
--More--
```

```
Dell# show ip interface brief
Interface                IP-Address      OK  Method Status
Protocol
TenGigabitEthernet 0/0   unassigned      NO  Manual administratively down down
TenGigabitEthernet 0/1   10.10.10.1      NO  Manual administratively down down
TenGigabitEthernet 0/2   unassigned      NO  Manual administratively down down
TenGigabitEthernet 0/3   unassigned      NO  Manual administratively down down
fortyGigE 0/4            unassigned      NO  Manual administratively down down
fortyGigE 0/8            unassigned      NO  Manual administratively down down
--More--
```

```
Dell# show ip interface configured
TenGigabitEthernet 0/0 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent
IP unicast RPF check is not supported
```

```
TenGigabitEthernet 0/1 is down, line protocol is down
Internet address is 10.10.10.1/24
Broadcast address is 10.10.10.255
Address determined by config file
IP MTU is 1500 bytes
Directed broadcast forwarding is disabled
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent
IP unicast RPF check is not supported
--More--
```

Usage Information The following describes the `show ip interface brief` command shown in the following example.

Fields	Description
Interface	Displays type of interface and the associated slot and port number.
IP-Address	Displays the IP address for the interface, if configured.
Ok?	Indicates if the hardware is functioning properly.
Method	Displays "Manual" if the configuration is read from the saved configuration.
Status	States whether the interface is enabled (up) or disabled (administratively down).
Protocol	States whether IP is enabled (up) or disabled (down) on the interface.

Example (Brief)

```
Dell#show ip int brief
Interface                IP-Address  OK? Method  Status                  Protocol
TenGigabitEthernet 1/0   unassigned  NO  Manual  administratively down down
TenGigabitEthernet 1/1   unassigned  NO  Manual  administratively down down
TenGigabitEthernet 1/2   unassigned  YES Manual  up                      up
TenGigabitEthernet 1/3   unassigned  YES Manual  up                      up
TenGigabitEthernet 1/4   unassigned  YES Manual  up                      up
TenGigabitEthernet 1/5   10.10.10.1  YES Manual  up                      up
TenGigabitEthernet 1/6   unassigned  NO  Manual  administratively down down
```

show ip management-route

View the IP addresses assigned to the Management interface.

C9000 Series

Syntax `show ip management-route [all | connected | summary | static]`

Parameters

all	(OPTIONAL) Enter the keyword `all` to view all IP addresses assigned to all Management interfaces on the switch.
connected	(OPTIONAL) Enter the keyword `connected` to view only routes directly connected to the Management interface.
summary	(OPTIONAL) Enter the keyword `summary` to view a table listing the number of active and non-active routes and their sources.
static	(OPTIONAL) Enter the keyword `static` to view non-active routes also.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip management-route

Destination     Gateway                   State
-----------     -------                   -----
10.1.2.0/24     ManagementEthernet 0/0    Connected
172.16.1.0/24   10.1.2.4                  Active
Dell#
```

show ipv6 management-route

Display the IPv6 static routes configured for the management interface.

C9000 Series

Syntax `show ipv6 management-route [all | connected | summary | static]`

Parameters

all	(OPTIONAL) Enter the keyword `all` to view all IP addresses assigned to all Management interfaces on the switch.
connected	(OPTIONAL) Enter the keyword `connected` to view only routes directly connected to the Management interface.
summary	(OPTIONAL) Enter the keyword `summary` to view a table listing the number of active and non-active routes and their sources.
static	(OPTIONAL) Enter the keyword `static` to view non-active routes also.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.4.1.0	Introduced on the C- and E-Series.
8.3.7.0	Introduced on the S4810.

Example

```
Dell#show ipv6 management-route
IPv6 Destination   Gateway                 State
----------------    -------                -----
2001:34::0/64      ManagementEthernet 0/0  Connected
2001:68::0/64      2001:34::16             Active
Dell#
```

show ip protocols

View information on all routing protocols enabled and active on the switch.

C9000 Series

Syntax `show ip protocols`

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Regular evaluation optimization enabled/disabled added to display output.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip protocols
Routing Protocol is "bgp 1"
  Cluster Id is set to 20.20.20.3
  Router Id is set to 20.20.20.3
  Fast-external-fallover enabled
  Regular expression evaluation optimization enabled
  Capable of ROUTE_REFRESH
  For Address Family IPv4 Unicast
   BGP table version is 0, main routing table version 0
   Distance: external 20 internal 200 local 200
   Neighbor(s):
     Address : 20.20.20.2
     Filter-list in : foo
     Route-map in : foo
     Weight : 0
   Address : 5::6
     Weight : 0
Dell#
```

show ip route

View information, including how they were learned, about the IP routes on the switch.

C9000 Series

Syntax

```
show ip route hostname | ip-address [mask] [longer-prefixes] | list prefix-list
| protocol [process-id | routing-tag] | all | connected | static | summary]
[vrf vrf-name]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the VRF name to list the routes in the route table of a specific VRF.
ip-address	(OPTIONAL) Specify a name of a device or the IP address of the device to view more detailed information about the route.
mask	(OPTIONAL) Specify the network mask of the route. Use this parameter with the IP address parameter.
longer-prefixes	(OPTIONAL) Enter the keywords `longer-prefixes` to view all routes with a common prefix.

list *prefix-list*	(OPTIONAL) Enter the keyword `list` and the name of a configured prefix list. For more information, refer to the show ip route list command.
protocol	(OPTIONAL) Enter the name of a routing protocol (`bgp`, `isis`, `ospf`, `rip`) or the keywords connected or static. **NOTE: `bgp`, `isis`, `ospf`, and `rip`.** • If you enter `bgp`, you can include the BGP *`as-number`* . • If you enter `isis`, you can include the ISIS *`routing-tag`*. • If you enter `ospf`, you can include the OSPF *`process-id`*.
process-id	(OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
routing-tag	(OPTIONAL) Specify that only ISIS routes with a certain routing tag must be displayed.
connected	(OPTIONAL) Enter the keyword `connected` to view only the directly connected routes.
all	(OPTIONAL) Enter the keyword `all` to view both active and non-active routes.
static	(OPTIONAL) Enter the keyword `static` to view only routes the `ip route` command configures.
summary	(OPTIONAL) Enter the keyword `summary`. For more information, refer to the show ip route summary command.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Added support for VRF.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.9.1.0	Introduced VRF on the E-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
pre-6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip route all

Codes:C- connected, S - static, R - RIP
      B- BGP, IN - internal BGP, EX - external BGP, LO - Locally Originated
      O- OSPF, IA - OSPF inter area N1 - OSPF NSSA external type 1
      N2- OSPF NSSA external type 2, E1 - OSPF external type 1
      E2- OSPF external type 2, i - IS-IS, L1 - IS-IS level-1
      L2- IS-IS level-2, IA - IS-IS inter area, * - candidate default
      >- non-active route + - summary route

Gateway of last resort is not set

     Destination     Gateway            Dist/Metric Last Change
----------- ------- ----------- -----------
R   3.0.0.0/8       via 100.10.10.10, So 2/8 120/1   00:07:12
                    via 101.10.10.10, So 2/9
    100.10.10.0/24  Direct, Te 2/8           0/0     00:08:54
> R 100.10.10.0/24  Direct, Te 2/8           120/0   00:08:54
C   101.10.10.0/24  Direct, Te 2/9           0/0     00:09:15
> R 101.10.10.0/24  Direct, Te 2/9           120/0   00:09:15
Dell#
```

Example (Summary)

```
Dell#show ip route summary

Route Source  Active Routes   Non-active Routes
connected     2               0
static        1               0
Total         3               0
Total 3 active route(s) using 612 bytes

Dell#show ip route static
Destination     Gateway                 Dist/Metric Last Change
-----------     -------                 ----------- -----------
*S  0.0.0.0/0   via 10.10.91.9, Te 1/2  1/0         3d2h
```

show ip route list

Display IP routes in an IP prefix list.

C9000 Series

Syntax

```
show ip route list prefix-list
```

Parameters

prefix-list	Enter the name of a configured prefix list.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show ip route list test

Codes:C- connected, S - static, R - RIP,
      B- BGP, IN - internal BGP, EX - external BGP,LO - Locally Originated,
      O- OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
      N2- OSPF NSSA external type 2, E1 - OSPF external type 1,
      E2- OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
      L2- IS-IS level-2, IA - IS-IS inter area, * - candidate default,
      >- non-active route, + - summary route

Gateway of last resort is not set

    Destination   Gateway             Dist/Metric Last Change
    -----------   -------             ----------- -----------
R   2.1.0.0/24    via 2.1.4.1, Te 2/43   120/2       3d0h
R   2.1.1.0/24    via 2.1.4.1, Te 2/43   120/2       3d1h
R   2.1.2.0/24    via 2.1.4.1, Te 2/43   120/1       3d0h
R   2.1.3.0/24    via 2.1.4.1, Te 2/43   120/1       3d1h
C   2.1.4.0/24    Direct, Te 2/43          0/0       3d1h
```

Related Commands

ip prefix-list — enters CONFIGURATION-IP PREFIX-LIST mode and configures a prefix list.

show ip prefix-list summary — displays a summary of the configured prefix lists.

show ip route summary

View a table summarizing the IP routes in the switch.

C9000 Series

Syntax

```
show ip route summary
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip route summary` shown in the following example.

Column Heading	Description
Route Source	Identifies how the route is configured in the system.
Active Routes	Identifies the best route if a route is learned from two protocol sources.
Non-active Routes	Identifies the back-up routes when a route is learned by two different protocols. If the best route or active route goes down, the non-active route becomes the best route.
ospf 100	If routing protocols (OSPF, RIP) are configured and routes are advertised, then information on those routes is displayed.
Total 1388 active...	Displays the number of active and non-active routes and the memory usage of those routes. If there are no routes configured in the system, this line does not appear.

Example

```
Dell>show ip route summary

Route Source   Active Routes   Non-active Routes
connected      17              0
static         3               0
ospf 100       1368            2
Intra-area: 762 Inter-area: 1 External-1: 600 External-2: 5
Total          1388            2
Total 1388 active route(s) using 222440 bytes
Total 2 non-active route(s) using 128 bytes
Dell>
```

Related Commands

show ip route — displays information about the routes found in the switch.

show ip traffic

View IP traffic statistics related to switch CPUs, including ICMP, UDP, TCP and ARP counters.

C9000 Series

Syntax

```
show ip traffic {all | cp | rp}
```

Parameters

all	(OPTIONAL) Enter the keyword `all` to view IP traffic statistics from all processors.
cp	(OPTIONAL) Enter the keyword `cp` to view only IP traffic statistics from the Control Processor.
rp	(OPTIONAL) Enter the keyword `rp` to view only IP traffic statistics from the Route Processor.

Default View IP traffic statistics from all processors.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The following describes the `show ip traffic` summary shown in the following example.

Keyword	Definition
unknown protocol...	No receiver for these packets. Counts packets whose protocol type field is not recognized by the system.
not a gateway...	Packets can not be routed; the host/network is unreachable.
security failures...	Counts the number of received unicast/multicast packets that could not be forwarded due to: • route not found for unicast/multicast; ingress interfaces do not belong to the destination multicast group

Keyword	Definition
	• destination IP address belongs to reserved prefixes; the host/network is unreachable
bad options...	Unrecognized IP option on a received packet.
Frags:	IP fragments received.
... reassembled	Number of IP fragments that were reassembled.
... timeouts	Number of times a timer expired on a reassembled queue.
... too big	Number of invalid IP fragments received.
... couldn't fragment	Number of packets that could not be fragmented and forwarded.
...encapsulation failed	Counts packets which could not be forwarded due to ARP resolution failure. The system sends an ARP request prior to forwarding an IP packet. If a reply is not received, the system repeats the request three times. These packets are counted in encapsulation failed.
Rcvd:	Total number of packets received from specified protocol.
...short packets	The number of bytes in the packet are too small.
...bad length	The length of the packet was not correct.
...no port broadcasts	The incoming broadcast/multicast packet did not have any listener.
...socket full	The applications buffer is full and the incoming packet are dropped.

The F10 Monitoring MIB provides access to the following statistics.

- **IP Statistics: Bcast: Received:** Object = f10BcastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.1
- **IP Statistics: Bcast: Sent:** Object = f10BcastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.2
- **IP Statistics: Mcast: Received:** Object = f10McastPktRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.3
- **IP Statistics: Mcast: Sent:** Object = f10McastPktSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.1.4
- **ARP Statistics: Rcvd: Request:** Object = f10ArpReqRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.1
- **ARP Statistics: Rcvd: Replies:** Object = f10ArpReplyRecv, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.3
- **ARP Statistics: Sent: Request:** Object = f10ArpReqSent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.2
- **ARP Statistics: Sent: Replies:** Object = f10ArpReplySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.4
- **ARP Statistics: Sent: Proxy:** Object = f10ArpProxySent, OIDs = 1.3.6.1.4.1.6027.3.3.5.2.5

Example

```
Dell#show ip traffic
Control Processor IP Traffic:

IP statistics:
  Rcvd: 23857 total, 23829 local destination
    0 format errors, 0 checksum errors, 0 bad hop count
    0 unknown protocol, 0 not a gateway
    0 security failures, 0 bad options
  Frags: 0 reassembled, 0 timeouts, 0 too big
    0 fragmented, 0 couldn't fragment
  Bcast: 28 received, 0 sent; Mcast: 0 received, 0 sent
  Sent: 16048 generated, 0 forwarded
    21 encapsulation failed, 0 no route
ICMP statistics:
  Rcvd: 0 format errors, 0 checksum errors, 0 redirects, 0 unreachable
    0 echo, 0 echo reply, 0 mask requests, 0 mask replies, 0 quench
    0 parameter, 0 timestamp, 0 info request, 0 other
  Sent: 0 redirects, 0 unreachable, 0 echo, 0 echo reply
    0 mask requests, 0 mask replies, 0 quench, 0 timestamp
    0 info reply, 0 time exceeded, 0 parameter problem
```

```
UDP statistics:
  Rcvd: 0 total, 0 checksum errors, 0 no port
    0 short packets, 0 bad length, 0 no port broadcasts, 0 socket full
  Sent: 0 total, 0 forwarded broadcasts
TCP statistics:
  Rcvd: 23829 total, 0 checksum errors, 0 no port
  Sent: 16048 total
ARP statistics:
  Rcvd: 156 requests, 11 replies
  Sent: 21 requests, 10 replies (0 proxy)
```

Related Commands clear ip traffic — clears IP traffic statistics.

show tcp statistics

Display statistical information about TCP traffic transmitted on Z9500 CPUs.

C9000 Series

Syntax `show tcp statistics {all | cp | rp}`

Parameters

all	Enter the keyword all to view `all` TCP statistics on the switch CPUs.
cp	Enter the keyword `cp` to view TCP statistics only from the Control Processor.
rp	Enter the keyword `rp1` to view TCP statistics only from the Route Processor.

Command Modes EXEC Privilege

Default Display TCP information from all processors.

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
6.4.1.0	Introduced

Usage Information The following describes the `show tcp statistics cp` command shown in the following example.

Field	Description
Rcvd:	Displays the number and types of TCP packets received by the switch.

Field	Description
	• Total = total packets received • no port = number of packets received with no designated port
0 checksum error...	Displays the number of packets received with the following: • checksum errors • bad offset to data • too short
329 packets...	Displays the number of packets and bytes received in sequence.
17 dup...	Displays the number of duplicate packets and bytes received.
0 partially...	Displays the number of partially duplicated packets and bytes received.
7 out-of-order...	Displays the number of packets and bytes received out of order.
0 packets with data after window	Displays the number of packets and bytes received that exceed the switch's window size.
0 packets after close	Displays the number of packet received after the TCP connection was closed.
0 window probe packets...	Displays the number of window probe and update packets received.
41 dup ack...	Displays the number of duplicate acknowledgement packets and acknowledgement packets with data received.
10184 ack...	Displays the number of acknowledgement packets and bytes received.
Sent:	Displays the total number of TCP packets sent and the number of urgent packets sent.
25 control packets...	Displays the number of control packets sent and the number retransmitted.
11603 data packets...	Displays the number of data packets sent.
24 data packets retransmitted	Displays the number of data packets resent.
355 ack..	Displays the number of acknowledgement packets sent and the number of packet delayed.
0 window probe...	Displays the number of window probe and update packets sent.
7 Connections initiated...	Displays the number of TCP connections initiated, accepted, and established.
14 Connections closed...	Displays the number of TCP connections closed, dropped.
20 Total rxmt...	Displays the number of times the switch tried to re-send data and the number of connections dropped during the TCP retransmit timeout period.
0 Keepalive....	Lists the number of keepalive packets in timeout, the number keepalive probes and the number of TCP connections dropped during keepalive.

Example

```
Dell#show tcp statistics cp

Control Processor TCP:
```

```
Rcvd: 10585 Total, 0 no port
   0 checksum error, 0 bad offset, 0 too short
   329 packets (1263 bytes) in sequence
   17 dup packets (6 bytes)
   0 partially dup packets (0 bytes)
   7 out-of-order packets (0 bytes)
   0 packets ( 0 bytes) with data after window
   0 packets after close
   0 window probe packets, 41 window update packets
   41 dup ack packets, 0 ack packets with unsend data
   10184 ack packets (12439508 bytes)
Sent: 12007 Total, 0 urgent packets
   25 control packets (including 24 retransmitted)
   11603 data packets (12439677 bytes)
   24 data packets (7638 bytes) retransmitted
   355 ack only packets (41 delayed)
   0 window probe packets, 0 window update packets
   7 Connections initiated, 8 connections accepted, 15 connections established
   14 Connections closed (including 0 dropped, 0 embryonic dropped)
   20 Total rxmt timeout, 0 connections dropped in rxmt timeout
   0 Keepalive timeout, 0 keepalive probe, 0 Connections dropped in keepalive
Dell#
```

Related Commands clear tcp statistics — clears TCP traffic statistics.

27

IPv6 Access Control Lists (IPv6 ACLs)

IPv6 ACLs and IPv6 Route Map commands are supported on Dell Networking operating system.

NOTE: For IPv4 ACL commands, refer to the Access Control Lists (ACL) chapter.

Important Points to Remember

- Certain platforms require manual CAM usage space allotment. For more information, see the cam-acl command.
- Egress IPv6 ACL and IPv6 ACL on the Loopback interface is not supported.
- Reference to an empty ACL permits any traffic.
- ACLs are not applied to self-originated traffic (for example, Control Protocol traffic not affected by IPv6 ACL because the routed bit is not set for Control Protocol traffic and for egress ACLs the routed bit must be set).
- You can use the same access list name for both IPv4 and IPv6 ACLs.
- You can apply both IPv4 and IPv6 ACLs on an interface at the same time.
- You can apply IPv6 ACLs on physical interfaces and a logical interfaces (Port-channel/VLAN).
- Non-contiguous masks are not supported in source or destination addresses in IPv6 ACL entries.
- Because the prefix mask is specified in /x format in IPv6 ACLs, inverse mask is not supported.

Topics:

- cam-acl
- cam-acl-egress
- clear counters ipv6 access-group
- deny (for IPv6 ACLs)
- deny icmp (for Extended IPv6 ACLs)
- deny tcp (for IPv6 ACLs)
- deny udp (for IPv6 ACLs)
- ipv6 access-list
- ipv6 control-plane egress-filter
- permit (for IPv6 ACLs)
- permit icmp (for IPv6 ACLs)
- permit tcp (for IPv6 ACLs)
- permit udp (for IPv6 ACLs)
- seq (for IPv6 ACLs)
- show cam-usage
- show ipv6 access-list
- show ipv6 accounting access-list
- show running-config

cam-acl

Allocate content addressable memory (CAM) for IPv4 and IPv6 ACLs.

C9000 Series

Syntax

```
cam-acl {default | l2acl number{ ipv4acl number ipv6acl number ipv4qos number
l2qos number l2pt number ipmacacl number vman-qos | vman-dual-qos number
ecfmacl number [ openflow number fcoeacl number | fedgovacl number|
nlbclusteracl number | ipv4pbr number | iscsioptaclnumber | openflow number |
vrfv4ac numberl ]}}
```

Parameters

default Use the default CAM profile settings and set the CAM as follows:

- L3 ACL (ipv4acl): 4
- L2 ACL(l2acl): 5
- IPv6 L3 ACL (ipv6acl): 0
- L3 QoS (ipv4qos): 2
- L2 QoS (l2qos): 1
- OpenFlow: 0 (disabled)
- FCoE (fcoeacl): 0 (disabled)
- iSCSI Optimization (iscsioptacl): 0 (disabled)
- L2 PT : 0
- IP-MAC ACL : 0
- Vman QoS : 0
- ECFM ACL: 0
- IPv4 PBR : 0
- VRFv4 ACL : 0
- FedGov ACL : 0
- NLB Cluster ACL : 0

l2acl *number* Allocate space to each CAM region.

Enter the CAM profile name then the amount for CAM space allocation. The total space allocated must be equal to 12. The IPv6 ACL range must be a factor of 2.

Enter `l2acl` and the FP block *number* for L2 ACL. The FP block number range is from 1 to 8.

- `4`: Creates 242 entries for use by the OpenFlow controller (256 total entries minus the 14 entries reserved for internal functionality)
- `8`: Creates 498 entries for use by the OpenFlow controller (512 total entries minus the 14 entries reserved for internal functionality)

ipv4acl *number* Enter `ipv4acl` and the FP block *number* for IPv4. The FP block number range is from 0 to 8.

ipv6acl *number* Enter `ipv6acl` and the FP block *number* for IPv6. The FP block number range is from 0 to 4 (multiples of 2).

ipv4qos *number* Enter `ipv4qos` and the FP block *number* for IPv4–QoS. The FP block number range is from 0 to 8.

l2qos *number* Enter `l2qos` and the FP block *number* for L2–QoS. The FP block number range is from 1 to 8.

l2pt *number* Enter `l2pt` and the FP block *number* for L2–Protocol tunneling. The FP block number range is from 0 to 1.

ipmacacl *number* Enter `ipmacacl` and the FP block *number* for IP-MAC ACL. The FP block number range is from 0 to 6.

vman-qos *number* Enter `vman-qos` and the FP block *number* for Vman QoS. The FP block number range is from 0 to 6.

ecfmacl *number* Enter `ecfmacl` and the FP block *number* for ECFM ACL. The FP block number range is from 0 to 5.

fcoeacl *number* Enter `fcoeacl` and the FP block *number* for FCoE ACL. The FP block number range is 0 to 6.

fedgovacl *number* Enter `fedgovacl` and the FP block *number* for Fed Gov ACL. The FP block number range is 0 to .

nlbclusteracl *number* Enter `nlbclusteracl` and the FP block *number* for NLB Cluster ACL. The FP block number range is 0 to 6.

ipv4pbr *number* Enter `ipv4pbr` and the FP block *number* for IPv4 PBR ACL. The FP block number range is 0 to 6.

iscsioptacl *number* Enter `iscsioptacl` and the FP block *number* for ISCSI optimization ACL. The FP block number range is 0 to 6.

openflow *number* Enter `openflow` and the FP block *number* for OpenFlow ACL. The FP block number range is 0 to 6.

vrfv4acl *number* Enter `vrfv4acl` and the FP block *number* for VRF ACL. The FP block number range is 0 to 6.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Added support for the `fcoe` parameter on the S4810 and S4820T.
9.1.(0.0)	Added support for OpenFlow on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Added the keywords `fcoeacl` and `iscsioptacl` on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Added the keywords `ecfmacl`, `vman-qos`, and `vman-dual-qos`.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.

Usage Information

For the new settings to take effect, save the new CAM settings to the startup-config (`write-mem` or `copy run start`) then reload the system.

The total amount of space allowed is 16 FP Blocks. System flow requires four blocks and these blocks cannot be reallocated. The total number of blocks must be equal to 12. The `ipv4acl` profile range is from 0 to 8.

When configuring space for IPv6 ACLs, the total number of Blocks must equal 12.

Ranges for the CAM profiles are from 1 to 10, except for the `ipv6acl` profile which is from 0 to 10. The `ipv6acl` allocation must be a factor of 2 (2, 4, 6, 8, 10).

If you enabled BMP 3.0, to perform a reload on the chassis to upgrade any configuration changes that have changed the NVRAM content, use the `reload conditional nvram-cfg-change` command.

You can use the `cam-acl default` command in Configuration Terminal Batch mode to reset ACL CAM entries to default settings in a dual-homing setup.

cam-acl-egress

Allocate space for IPv6 egress ACLs.

C9000 Series

Syntax `cam-acl-egress {default | l2acl` *1-3* `ipv4acl` *1-3* `ipv6acl` *0-2*`}`

Parameters

default Use the default CAM profile settings, and set the CAM as follows:

- L2 ACL(l2acl): **1**
- L3 ACL (ipv4acl: **1**
- IPv6 L3 ACL (ipv6acl): **2**

l2acl *1-3* **ipv4acl** *1- 3* **ipv6acl** *0-2*	Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the allocation amount. The `ipv6acl` range must be a factor of 2.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.2.0	Introduced on the E-Series TeraScale.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.

Usage Information

For the new settings to take effect, save the new CAM settings to the startup-config (`write-mem` or `copy run start`), then reload the system.

You can use the `cam-acl-egress` command in Configuration Terminal Batch mode to allocate space for egress ACLs in a dual-homing setup.

Example

```
Dell#
Dell#configure
Dell(conf)#cam-acl-egress ?
default      Reset Egress CAM ACL entries to default setting
l2acl        Set L2-ACL entries
Dell(conf)#cam-acl-egress l2acl ?
<1-3>        Number of FP blocks for l2acl
Dell(conf)#cam-acl-egress l2acl 1 ?
ipv4acl      Set IPV4-ACL entries
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ?
ipv6acl      Set IPV6-ACL entries
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl ?
<0-2>        Number of FP blocks for IPV6 (multiples of 2)
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl 2
```

clear counters ipv6 access-group

Erase all counters maintained for the IPv6 access lists.

C9000 Series

Syntax `clear counters ipv6 access-group [access-list-name]`

Parameters

access-list-name	(OPTIONAL) Enter the name of a configured access-list, up to 140 characters.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.
8.2.1.0	Introduced on the E-Series TeraScale.
7.8.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series TeraScale Added the `monitor` option.

deny (for IPv6 ACLs)

Configure a filter that drops IPv6 packets matching the filter criteria.

C9000 Series

Syntax `deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp}` command

Parameters

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.

threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the `seq`, `permit`, or deny commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based `enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny icmp (for Extended IPv6 ACLs)

Configure a filter to drop all or specific ICMP messages.

C9000 Series

NOTE: Only the options that have been newly introduced in Release 9.3(0.0) and Release 9.4(0.0) are described here. For a complete description on all of the keywords and variables that are available with this command, refer the topic of this command discussed earlier in this guide.

Syntax

`deny icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [message-type] [count [byte]] | [log [interval minutes] [threshold-in-msgs [count]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command

Parameters

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the seq, permit, or deny commands. You can enter a threshold in the range of 1-100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. You can enter an interval in the range of 1-10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is 5 minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3.0.0	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet

count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny tcp (for IPv6 ACLs)

Configure a filter that drops TCP packets that match the filter criteria.

C9000 Series

Syntax

```
deny tcp {source address mask | any | host ipv6-address} [operator port [port]]
{destination address | any | host ipv6-address} [bit] [operator port [port]]
[count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny tcp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command

Parameters

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the seq, permit, or deny commands. The threshold range is from 1 to 100..
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The time interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based enable command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

deny udp (for IPv6 ACLs)

Configure a filter to drop user datagram protocol (UDP) packets meeting the filter criteria.

C9000 Series

Syntax

```
deny udp {source address mask | any | host ipv6-address} [operator port [port]]
{destination address | any | host ipv6-address} [operator port [port]] [count
[byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no deny udp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command

Parameters

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the seq, permit, or deny commands. The threshold range is from 1 to 100.

interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The threshold range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Command Modes ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, Z9000, and MXL 10/40GbE Switch IO Module platforms.
9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, Z9000, and MXL 10/40GbE Switch IO Module platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs.

You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the flow-based `enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

ipv6 access-list

Configure an access list based on IPv6 addresses or protocols.

C9000 Series

Syntax `ipv6 access-list` *`access-list-name`*

To delete an access list, use the `no ipv6 access-list` *`access-list-name`* command.

Parameters

access-list-name	Enter the access list name as a string, up to 140 characters.

Defaults All access lists contain an implicit "deny any"; that is, if no match occurs, the packet is dropped.

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series. Increased the name string to accept up to 140 characters. Prior to version 7.8.1.0, names are up to 16 characters long.
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information The number of entries allowed per ACL is hardware-dependent. For detailed specification on entries allowed per ACL, refer to your line card documentation.

Use this command in Configuration Terminal Batch mode to configure the access list in a dual-homing setup.

Related Commands show config — views the current configuration.

ipv6 control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv6 CPU traffic.

C9000 Series

Syntax `ipv6 control-plane egress-filter`

Defaults Not enabled.

Command Modes EXEC Privilege

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.

permit (for IPv6 ACLs)

Configure a filter that matches the filter criteria, select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP.

C9000 Series

Syntax

`permit {`*`ipv6-protocol-number`* `| icmp | ipv6 | tcp | udp} [count [byte]] [dscp` *`value`*`] [order] [fragments] [log [interval` *`minutes`*`] [threshold-in-msgs [`*`count`*`]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command syntax if you know the filter's sequence number
- Use the `no permit {`*`ipv6-protocol-number`* `| icmp | ipv6 | tcp | udp}` command

Parameters

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the`flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

permit icmp (for IPv6 ACLs)

Allow filtering of all or specific internet control message protocol (ICMP) messages

C9000 Series

Syntax

`permit icmp {`*`source address mask`*` | any | host `*`ipv6-address`*`} {`*`destination address`*` | any | host `*`ipv6-address`*`} [`*`message-type`*`] [count [byte]] [log [interval `*`minutes`*`] [threshold-in-msgs [`*`count`*`]] [monitor]`

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit icmp {`*`source address mask`*` | any | host `*`ipv6-address`*`} {`*`destination address`*` | any | host `*`ipv6-address`*`}` command.

Parameters

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.

monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the`flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is very useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

permit (for Standard IPv6 ACLs) – configures a filter to forward IPv6 packets.

permit tcp (for IPv6 ACLs)

Configure a filter to pass TCP packets that match the filter criteria.

C9000 Series

Syntax

```
permit tcp {source address mask | any | host ipv6-address} [operator port
[port]] {destination address | any | host ipv6-address} [bit] [operator port
```

[*port*]] [count [byte]] [log [interval *minutes*] [threshold-in-msgs [*count*]] [monitor]

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit tcp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated. with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults

By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is 5 minutes. By default, flow-based monitoring is not enabled.

Command Modes

ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introducued on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists.

This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands permit (for Standard IPv6 ACLs) – configures a filter to forward IPv6 packets.

permit udp (for IPv6 ACLs)

Configure a filter to pass UDP packets meeting the filter criteria.

C9000 Series

Syntax

```
permit udp {source address mask | any | host ipv6-address} [operator port
[port]] {destination address | any | host ipv6-address} [operator port [port]]
[count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, you have two choices:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- Use the `no permit udp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address}` command.

Parameters

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminated with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Command Modes ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3.0.0	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands permit (for Standard IPv6 ACLs) – configures a filter to forward IPv6 packets.

seq (for IPv6 ACLs)

Assign a sequence number to a deny or permit the filter in an IPv6 access list while creating the filter.

C9000 Series

Syntax

```
seq sequence-number {deny | permit} {ipv6-protocol-number | icmp | ip | tcp | udp} {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [operator port [port]] [count [byte]] [log [interval minutes] [threshold-in-msgs [count]] [monitor]
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

log	(OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.
threshold-in msgs *count*	(OPTIONAL) Enter the `threshold-in-msgs` keyword followed by a value to indicate the maximum number of ACL logs that can be generated, exceeding which the generation of ACL logs is terminate with the `seq`, `permit`, or `deny` commands. The threshold range is from 1 to 100.
interval *minutes*	(OPTIONAL) Enter the keyword `interval` followed by the time period in minutes at which ACL logs must be generated. The interval range is from 1 to 10 minutes.
monitor	(OPTIONAL) Enter the keyword `monitor` when the rule is describing the traffic that you want to monitor and the ACL in which you are creating the rule is applied to the monitored interface.

Defaults By default, 10 ACL logs are generated if you do not specify the threshold explicitly.

The default frequency at which ACL logs are generated is five minutes. By default, flow-based monitoring is not enabled.

Command Modes ACCESS-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.

Usage Information

When the configured maximum threshold is exceeded, generation of logs is stopped. When the interval at which ACL logs are configured to be recorded expires, the subsequent, fresh interval timer is started and the packet count for that new interval commences from zero. If ACL logging was stopped previously because the configured threshold is exceeded, it is re-enabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is re-enabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, IPv6 ACLs, and MAC ACLs. You can configure ACL logging only on ACLs that are applied to ingress interfaces; you cannot enable logging for ACLs that are associated with egress interfaces.

You can activate flow-based monitoring for a monitoring session by entering the `flow-based enable` command in the Monitor Session mode. When you enable this capability, traffic with particular flows that are traversing through the ingress and egress interfaces are examined and, appropriate ACLs can be applied in both the ingress and egress direction. Flow-based monitoring conserves bandwidth by monitoring only specified traffic instead all traffic on the interface. This feature is particularly useful when looking for malicious traffic. It is available for Layer 2 and Layer 3 ingress and egress traffic. You may specify traffic using standard or extended access-lists. This mechanism copies all incoming or outgoing packets on one port and forwards (mirrors) them to another port. The source port is the monitored port (MD) and the destination port is the monitoring port (MG).

Related Commands

permit (for Standard IPv6 ACLs) – configures a filter to forward IPv6 packets.

show cam-usage

Display the amount of memory space used and available in each CAM partition (including Layer 2 ACL, Layer 3 ACL, and IPv4Flow).

Syntax

```
show cam-usage [acl | router | switch]
```

Parameters

acl	(OPTIONAL) Enter the keyword `acl` to display Layer 2 and Layer 3 ACL CAM usage.
router	(OPTIONAL) Enter the keyword `router` to display Layer 3 CAM usage.
switch	(OPTIONAL) Enter the keyword `switch` to display Layer 2 CAM usage.

Command Modes

EXEC

EXEC Privilege

Command History

Version	Description
9.11.0.0	The `show cam-usage` command is updated to display ECMP group count information.
9.5.(0.0)	Introduced on the Z9500.
9.3.(0.0)	Introduced on the S4810, S4820T, Z9000 and MXL.

Usage Information

The following regions must be provided in the `show cam-usage` output:

- L3AclCam
- L2AclCam
- V6AclCam

The following table describes the output fields of the `show cam-usage` command.

Table 5. Output fields of the show cam-usage command

Field	Description
LineCard	Number of the line card that contains information on ACL VLAN groups
Portpipe	The hardware path that packets follow through a system for ACL optimization
CAM-Region	Type of area in the CAM block that is used for ACL VLAN groups
Total CAM space	Total amount of space in the CAM block
Used CAM	Amount of CAM space that is currently in use
Available CAM	Amount of CAM space that is free and remaining to be allocated for ACLs

Example 1: Output of the show cam-usage Command

```
Stackunit|Portpipe| CAM Partition   | Total CAM   |  Used CAM   |Available CAM
========|========|=================|=============|=============|==============
    1   |   0    | IN-L2 ACL       |      1008   |       320   |       688
        |        | IN-L2 FIB       |     32768   |      1132   |     31636
        |        | IN-L3 ACL       |     12288   |         2   |     12286
        |        | IN-L3 ECMP GRP  |      1024   |         0   |      1024
        |        | IN-L3 FIB       |    262141   |        14   |    262127
        |        | IN-L3-SysFlow   |      2878   |        45   |      2833
        |        | IN-L3-TrcList   |      1024   |         0   |      1024
        |        | IN-L3-McastFib  |      9215   |         0   |      9215
        |        | IN-L3-Qos       |      8192   |         0   |      8192
        |        | IN-L3-PBR       |      1024   |         0   |      1024
        |        | IN-V6 ACL       |         0   |         0   |         0
        |        | IN-V6 FIB       |         0   |         0   |         0
        |        | IN-V6-SysFlow   |         0   |         0   |         0
        |        | IN-V6-McastFib  |         0   |         0   |         0
        |        | OUT-L2 ACL      |      1024   |         0   |      1024
        |        | OUT-L3 ACL      |      1024   |         0   |      1024
        |        | OUT-V6 ACL      |         0   |         0   |         0
    1   |   1    | IN-L2 ACL       |       320   |         0   |       320
        |        | IN-L2 FIB       |     32768   |      1136   |     31632
        |        | IN-L3 ACL       |     12288   |         2   |     12286
        |        | IN-L3 FIB       |    262141   |        14   |    262127
        |        | IN-L3-SysFlow   |      2878   |        44   |      2834
--More--
```

Example 2: Output of the show cam-usage acl Command

```
Dell#show cam-usage acl
Stackunit|Portpipe| CAM Partition    | Total CAM   |  Used CAM   |Available CAM
========|========|==================|=============|=============|============
   11    |   0    | IN-L2 ACL        |      1008   |          0  |      1008
         |        | IN-L3 ACL        |     12288   |          2  |     12286
         |        | OUT-L2 ACL       |      1024   |          2  |      1022
         |        | OUT-L3 ACL       |      1024   |          0  |      1024
         |        | IN-L3 ECMP GRP   |      1024   |          0  |      1024
```

Example 3: Output of the show cam-usage router Command

Example 4: Output of the show cam-usage switch Command

show ipv6 access-list

Display IPv6 access-list information.

C9000 Series

Syntax `show ipv6 access-list { [name] | interface } { in | out | interface }`

Parameters

access-list	Enter the keywords `access-list` to display information for all ipv6 access-lists.
acl_name	Enter the keywords `acl_name` to display information for a specified ipv6 access-list.
in	Enter the keyword `in` to display information for an ipv6 ingress access-list attached to an interface.
out	Enter the keyword `out` to display information for an ipv6 egress access-list attached to an interface.
interface	Enter the keyword `interface` to display information for an ipv6 access-list for a specific interface.

Defaults None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information No output displays If you do not attach an ingress or egress access-list to an interface and you return to the `DELL#` prompt.

Example

```
Dell#show ipv6 access-list V6-ACL in
Ingress IPV6 access list V6-ACL
 seq 5 permit tcp any any count (0 packets)
 seq 10 permit udp any any count (0 packets)
Dell#
```

show ipv6 accounting access-list

View the IPv6 access-list and the sequence of filters.

C9000 Series

Syntax `show ipv6 accounting {access-list` *`access-list-name`* `| cam_count} interface` *`interface`*

Parameters

access-list-name	Enter the name of the ACL that you want to display. The ACL name size is limited to 140 characters.
cam_count	List the count of the CAM rules for this ACL.
interface *interface*	Enter the keyword `interface` and the interface type and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` a port channel number.The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` and the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` and the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.4.2.1	Introduced on the S-Series.
8.2.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.8.1.0	Introduced on the C-Series. Increased the name string to accept up to 140 characters. Prior to version 7.8.1.0, names are up to 16 characters long.
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information

Field	Description
"Ingress IPv6..."	Displays the name of the IPv6 ACL, in this Example "AclList1".
"seq 10..."	Displays the filter. If the keywords `count` or `byte` were configured in the filter, the number of packets or bytes processed by the filter is displayed at the end of the line.

Example

```
Dell#show ipv6 accounting access-list
!
Ingress IPv6 access list V6-ACL on TenGigabitEthernet 10/1
Total cam count 2
 seq 5 permit tcp any any count (0 packets)
 seq 10 permit udp any any count (0 packets)
```

show running-config

Display the ACL running configurations.

C9000 Series

Syntax

```
show running-config {acl [ip | mac | ipv6]}
```

Parameters

acl	Enter the keyword `acl` to display all access-lists and acl sub commands.
ip	Enter the keyword `ip` to display all ip access-list and the ip sub commands.
ipv6	Enter the keyword `ipv6` to display all ipv6 access-lists and ipv6 sub commands.
mac	Enter the keyword `mac` to display all L2 access-lists and sub commands.

Defaults None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Comma*

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Example

```
Dell# show running-config acl
ip
ip access-list standard five
seq 5 permit any
!
ip access-list standard four
 seq 5 permit any count bytes
```

```
 seq 10 deny any count

 seq 20 deny host 2.2.2.2 log threshold-in-msgs 10 interval 5
 !
show running-config acl  mac

mac access-list standard mac
seq 5 permit 11:22:33:44:55:66 count
 seq 10 deny any log threshold-in-msgs 10 interval 5 order 1
 seq 15 permit any order 2 monitor
!
```

28

IPv6 Basics

IPv6 basic commands are supported on the Dell Networking operating system.

NOTE: For information about the Dell Networking operating software version and platform that supports IPv6 in each software feature, refer to the *IPv6 Addressing* chapter of the *Dell Networking OS Configuration Guide*.

Topics:

- cam-ipv6 extended-prefix
- clear ipv6 fib
- clear ipv6 mld_host
- clear ipv6 neighbors
- ipv6 address
- ipv6 address autoconfig
- ipv6 address eui64
- ipv6 control-plane icmp error-rate-limit
- ipv6 flowlabel-zero
- ipv6 host
- ipv6 name-server
- ipv6 nd dad attempts
- ipv6 nd disable-reachable-timer
- ipv6 nd dns-server
- ipv6 nd prefix
- ipv6 neighbor
- ipv6 route
- ipv6 unicast-host-route
- ipv6 unicast-routing
- show cam-ipv6 extended-prefix
- show ipv6 cam linecard
- show ipv6 control-plane icmp
- show ipv6 fib linecard
- show ipv6 flowlabel-zero
- show ipv6 interface
- show ipv6 mld_host
- show ipv6 neighbors
- show ipv6 route

cam-ipv6 extended-prefix

Enable LPM CAM partitioning to support the storage of extended IPv6 (/65 to /128) route prefixes in LPM partition 1.

C9000 Series

Syntax

```
cam-ipv6 extended-prefix max-ipv6-prefixes
```

To remove LPM partitioning configuration, use no cam-ipv6 extended-prefix.

Parameters

max-ipv6-prefixes	Maximum number of extended IPv6 prefixes with the mask length of /65 to /128 that are supported in the LPM partition. The possible values are 1024, 2048, and 3072.

Defaults

LPM CAM is not partitioned with Partition 1. IPv6 /65 to /128 prefixes are not converted to /64 prefixes and saved in the LPM table. All the packets for extended IPv6 route prefixes are transmitted using the default route path.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.3(0.1)	Introduced on the S6000.

Usage Information

You can partition the LPM table to store extended IPv6 route prefixes with /65 to /128 mask lengths. LPM CAM partitioning requires a switch reload to take effect.

To disable LPM CAM partitioning and return the number of the IPv6 /65-/128 route prefixes stored in Partition 1 to 0, enter the `no cam-ipv6 extended-prefix` command.

clear ipv6 fib

Clear (refresh) all forwarding information base (FIB) entries on a line card.

C9000 Series

Syntax

```
clear ipv6 fib {linecard slot-id } vrf vrf-name
```

Parameters

vrf *vrf–name*	(Optional) Enter the keyword vrf followed by the name of the VRF to clear the neighbor corresponding to that VRF.

NOTE: If you do not specify this option, neighbors corresponding to the default VRF are cleared.

linecard *slot*	Enter the slot number to clear the FIB for a linecard. Range is 0 to 11.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

clear ipv6 mld_host

Clear the IPv6 MLD host counters and reset the elapsed time.

C9000 Series

Syntax `clear ipv6 mld_host`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Version	Description
8.3.11.1	Introduced on the Z9000.

clear ipv6 neighbors

Delete all entries in the IPv6 neighbor discovery cache or neighbors of a specific interface. Static entries are not removed using this command.

C9000 Series

Syntax

```
clear ipv6 neighbors [ipv6 address] | interface interface | vrf vrf name]
```

Parameters

ipv6-address — Enter the IPv6 address of the neighbor in the x:x:x:x::x format to remove a specific IPv6 neighbor.

NOTE: The :: notation specifies successive hexadecimal fields of zero.

vrf *vrf-name* — (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to clear the neighbor corresponding to that VRF.

NOTE: If you do not specify this option, the neighbors in the default VRF are cleared.

interface *interface* — To remove all neighbor entries learned on a specific interface, enter the keyword `interface` then the interface type and slot/port or number information of the interface:

Enter one of the following keywords with slot/port or number to clear information about the IPv6 neighbors learned on the specified interface:

- For a 1–Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information
- For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port-channel interface, enter the keyword `port-channel` with a port-channel number. The range of port-channel numbers is from 1 to 4096.
- For a VLAN interface, enter the keyword`vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel`.

Command Modes

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Added support for VRF.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

ipv6 address

Configure an IPv6 address to an interface.

C9000 Series

Syntax

`ipv6 address {ipv6-address prefix-length}`

To remove the IPv6 address, use the `no ipv6 address {ipv6-address prefix-length}` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults

none

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Updated Usage Information.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Added support on the management Ethernet port.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.

Version	Description
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information

- If two addresses are configured, delete an existing address before configuring a new address.
- If the last manually-configured global IPv6 address is removed using the "no" form of the command, the link-local IPv6 address is removed automatically.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

NOTE: Do not use the /128 prefix length on physical or port channel interfaces. You can use the /128 prefix length on loopback interfaces.

Example

```
Dell(conf)#interface tengigabitethernet 1/0
Dell(conf-if-te-1/0)#ipv6 address ?
X:X:X:X::X IPv6 address
Dell(conf-if-te-1/0)#ipv6 address 2002:1:2::3 ?
<0-128> Prefix length in bits
Dell(conf-if-te-1/0)#ipv6 address 2002:1:2::3 /96 ?
<cr>
Dell(conf-if-te-1/0)#ipv6 address 2002:1:2::3 /96
Dell(conf-if-te-1/0)#show config
!
interface TenGigabitEthernet 1/0
  no ip address
  ipv6 address 2002:1:2::3 /96
  no shutdown
Dell(conf-if-te-1/0)#
```

ipv6 address autoconfig

Configure IPv6 address auto-configuration for the management interface.

C9000 Series

Syntax

`ipv6 address autoconfig`

To disable the address autoconfig operation on the management interface, use the `no ipv6 address autoconfig` command.

Default

Disabled

Command Modes

INTERFACE (management interface only)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.1.(0.0)	Updated Usage Information section.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Infomation

- SAA can configure up to two addresses. If any preferred prefix or valid timers time out, the corresponding address are deprecated or removed. If an address is removed due to a time-out, an address from the current unused prefix is used to create a new address. If there are no remaining prefixes, the software waits to receive a new prefix from the RA.
- If auto-configuration is enabled, all IPv6 addresses on that management interface are auto-configured. Manual and auto-configurations are not supported on a single management interface.
- Removing auto-configuration removes all auto-configured IPv6 addresses and the link-local IPv6 address from that management interface.
- IPv6 addresses on a single management interface cannot be members of the same subnet.
- IPv6 secondary addresses on management interfaces across a platform must be members of the same subnet.
- IPv6 secondary addresses on management interfaces should not match the virtual IP address and should not be in the same subnet as the virtual IP.

ipv6 address eui64

Configure IPv6 EUI64 address configuration on the interface.

C9000 Series

Syntax

`ipv6 address {ipv6-address prefix-length} eui64`

To disable IPv6 EUI64 address autoconfiguration, use the `no ipv6 address {ipv6-address prefix-length} eui64` command.

Parameters

ipv6-address prefix-length	Enter the IPv6 prefix in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced.

Usage Information This command allows you to create an EUI64 address based on the specified prefix and MAC address only. Prefixes may be configured on the interface using the `ipv6 nd prefix` command without creating an EUI64 address.

Example

```
Dell(conf)#int ten 0/4
Dell(conf-if-te-0/4)#ipv6 address 200:1::/64 eui64
Dell(conf)#int ten 0/6
Dell(conf-if-te-0/6)#ipv6 address 801:10::/64 eui64
```

ipv6 control-plane icmp error-rate-limit

Configure the maximum number of ICMP error packets generated and sent in one second.

C9000 Series

Syntax `ipv6 control-plane icmp error-rate-limit {1-200}`

To restore the default value, use the `no ipv6 control-plane icmp error-rate-limit` command.

Parameters

pps	Enter the maximum number of error packets generated per second. The range is from 1 to 200.

Default 100 pps

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

ipv6 flowlabel-zero

Configure system to set the flow label field in the packets to zero.

C9000 Series

Syntax

`ipv6 flowlabel-zero`

To remove 0 from the flow label field and allow the protocol operations to fill the field, use the `no ipv6 flowlabel-zero` command.

Default

Disabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information

If the flowlabel value is already set for BGP or SSH, the system defaults to the already configured value. All packets on the same connection are considered part of the same flow by the system. For new connections, set the new flowlabel to zero.

ipv6 host

Assign a name and IPv6 address for the host-to-IPv6 address mapping table.

C9000 Series

Syntax

`ipv6 host name` *`ipv6-address`*

To remove an IP host, use the `no ipv6 host name {ipv6-address}`.

Parameters

name	Enter a text string to associate with one IP address.
ipv6-address	Enter the IPv6 address (X:X:X:X::X) to be mapped to the name.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.1.0	Introduced on the E-Series TeraScale.

ipv6 name-server

Enter up to six IPv6 addresses of name servers. The order you enter the addresses determines the order of their use.

C9000 Series

Syntax `ipv6 name-server` *`ipv6-address`* `[`*`ipv6-address2... ipv6-address6`*`]`

To remove a name server, use the `no ipv6 name–server ipv6-address` command.

Parameters

ipv6-address	Enter the IPv6 address (X:X:X:X::X) of the name server to be used. Note: The :: notation specifics successive hexadecimal fields of zeros.
ipv6-address2... *ipv6-address6*	(OPTIONAL) Enter up to five more IPv6 addresses, in the x:x:x:x::x format, of name servers to be used. Separate the IPv6 addresses with a space.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.1.0	Introduced on the E-Series TeraScale.

Usage Information You can separately configure both IPv4 and IPv6 domain name servers.

ipv6 nd dad attempts

Configure the number of neighbor solicitation messages that are sent to perform duplicate address detection (DAD) on the interface.

C9000 Series

Syntax `ipv6 nd dad attempts {number of attempts}`

To restore the default value, use the `no ipv6 nd dad attempts` command.

Parameters

number of attempts Enter the number of attempts to be made to detect a duplicate address. The range is from 0 to 15. Setting the value to 0 disables DAD on the interface.

Default 3 attempts

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

ipv6 nd disable-reachable-timer

Keep the learnt neighbor discovery entries stateless so that the entries do not time out.

Syntax

```
ipv6 nd disable-reachable-timer
```

To restore to default, use the `no ipv6 nd disable-reachable-timer` command.

Default Disabled

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11.0.1	Introduced on the S3100 series, S3048–ON, S4048–ON, S4048T-ON, S4810, S4820, S5000, S6000, S6010–ON, S6000–ON, S6100–ON, Z9100–ON, C9010, Z9500, MXL, and FN IOM.

ipv6 nd dns-server

Configure Recursive DNS Server (RDNSS) addresses for distribution via IPv6 router advertisements to an IPv6 device.

C9000 Series

Syntax

```
ipv6 nd dns-server {ipv6-RDNSS-address} {lifetime | infinite}
```

To remove the IPv6 RDSS configuration, use `no ipv6 nd dns-server {ipv6-RDNSS-address} {lifetime | infinite}`

Parameters

ipv6-RDNSS-address	Enter the IPv6 Recursive DNS Server's (RDNSS) address. You can specify up to 4 IPv6 RDNSS server addresses.
lifetime	Enter the lifetime in seconds. The amount of time the IPv6 host can use the IPv6 RDNSS address for name resolution. The range is `0` to `4294967295` seconds. When you specify the maximum lifetime value of `4294967295` or `infinite`, the lifetime does not expire. A value of `0` indicates to the host that the RDNSS address should not be used. You must specify a lifetime using the `lifetime` or `infinite` parameter.
infinite	Enter the keyword `infinite` to specify that the RDNSS lifetime does not expire.

Defaults Not Configured

Command Modes INTERFACE

INTERFACE (BATCH MODE)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information

Use the `ipv6 nd dns-server` command to add, edit, or delete an IPv6 RDNSS address and lifetime value. You can configure up to four IPv6 RDNSS addresses. You must specify a lifetime using the lifetime or infinite parameter. In the Configuration Terminal Batch mode, you can use this command to configure the IPv6 addresses in a dual-homing setup.

Example

```
Dell(conf-if-te-0/1)#ipv6 nd dns-server 1000::1 1
```

ipv6 nd prefix

Specify which IPv6 prefixes are included in Neighbor Advertisements.

C9000 Series

Syntax

```
ipv6 nd prefix {ipv6-prefix | prefix-length | default} [no-advertise] | [no-autoconfig] [no-rtr-address] [off-link] [lifetime {valid | infinite} {preferred | infinite}]
```

Parameters

ipv6-prefix	Enter an IPv6 prefix.
prefix-length	Enter the prefix then the prefix length. The length range is from 0 to 128.
default	Enter the keyword `default` to set default parameters for all prefixes.
no-advertise	Enter the keyword `no-advertise` to prevent the specified prefix from being advertised.
no-autoconfig	Enter the keywords `no-autoconfig` to disable Stateless Address Autoconfiguration.
no-rtr-address	Enter the keyword `no-rtr-address` to exclude the full router address from router advertisements (the R bit is not set).
off-link	Enter the keywords `off-link` to advertise the prefix without stating to recipients that the prefix is either on-link or off-link.
valid-lifetime | infinite	Enter the amount of time that the prefix is advertised, or enter `infinite` for an unlimited amount of time. The range is from 0 to 4294967295. The default is **2592000**. The maximum value means that the preferred lifetime does not expire for the valid-life time parameter.
preferred-lifetime | infinite	Enter the amount of time that the prefix is preferred, or enter `infinite` for an unlimited amount of time. The range is from 0 to 4294967295. The default is **604800**. The maximum value means that the preferred lifetime and does not expire.

Command Modes

INTERFACE

INTERFACE (BATCH MODE)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.2.0	Introduced on the E-Series TeraScale, C-Series, and S-Series.

Usage Information

By default, all prefixes configured as addresses on the interface are advertised. This command allows control over the individual parameters per prefix; you can use the `default` keyword to use the default parameters for all prefixes. If a prefix has been configured with lifetime parameter values, the default values cannot be applied using the `ipv6 nd prefix default no-autoconfig` command. Use this command in the Configuration Terminal Batch mode to advertise in a dual-homing setup.

ipv6 neighbor

Configure a static entry in the IPv6 neighbor discovery.

C9000 Series

Syntax

`ipv6 neighbor{`*`ipv6-address`*`} {interface `*`interface`*`} {`*`hardware_address`*`}[vrf `*`vrf-name`*`]`

To remove a static IPv6 entry from the IPv6 neighbor discovery, use the `no ipv6 neighbor`*`ipv6-address`*`{interface `*`interface`*

Parameters

ipv6-address Enter the IPv6 address of the neighbor in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zero.

interface *intehardware_rface* Enter the keyword `interface` then the interface type and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port/subport information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a Null interface, enter the keyword null then the Null interface number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number. The range is from 1 to 16383.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

hardware_address	Enter a 48-bit hardware MAC address in nn:nn:nn:nn:nn:nn format.
vrf *vrf-name*	(Optional) Enter the keyword vrf and the name of the VRF to install IPv6 routes in that VRF.

Defaults none

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

Usage Information Neighbor Discovery Protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. It defines mechanisms for solving problems, such as:

- Router discovery: Hosts can locate routers residing on a link

- Prefix discovery: Hosts can discover address prefixes for the link.
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination· Neighbor Unreachability Detection (NUD): Determine that a neighbor is no longer reachable on the link
- Duplicate Address Detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.

Use the ipv6 neighbor command to manually configure the IPv6 address of a neighbor to be discovered by the switch.

NOTE: The parameters vrf, mac-address, interface are not supported in the batch mode.

ipv6 route

Establish a static IPv6 route.

C9000 Series

Syntax

`ipv6 route` *`ipv6-address prefix-length`* `{`*`ipv6-address`* `|` *`interface`* `|` *`interface ipv6-address`*`} [`*`distance`*`] [tag` *`value`*`] [permanent][weight` *`weight-value`* `[vrf` *`vrf-name`*`]`

To remove the IPv6 route, use the `no ipv6 route` *`ipv6-address prefix-length`* `{`*`ipv6-address | interface | interface ipv6-address`*`} [`*`distance`*`] [tag` *`value`*`] [permanent][weight` *`weight-value`* `[vrf` *`vrf-name`*`]` command.

Parameters

ipv6-address prefix-length — Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

interface — (OPTIONAL) Enter the following keywords and slot/port or number information:

- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Null interface, enter the keyword null then the Null interface number.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number. The range is from 1 to 16383.
- For a VLAN interface, enter the keyword `VLAN` then the vlan number. The range is from 1 to 4094.

If you configure a static IPv6 route using an egress interface and enter the `ping` command to reach the destination IPv6 address, the ping operation may not work.

	Configure the IPv6 route using a next-hop IPv6 address in order for the `ping` command to detect the destination address.
ipv6-address	Enter the forwarding router IPv6 address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
distance	(OPTIONAL) Enter a number as the metric distance assigned to the route. The range is from 1 to 255.
tag *value*	(OPTIONAL) Enter the keyword `tag` then a tag value number. The range is from 1 to 4294967295.
permanent	(OPTIONAL) Enter the keyword `permanent` to specify that the route is not to be removed, even if the interface assigned to that route goes down. **NOTE: If you disable the interface with an IPv6 address associated with the keyword `permanent`, the route disappears from the routing table.**
weight *weight-value*	Enter the keyword `weight` followed by a weight value. The range is from 0 to 255. **NOTE: Weight for a static route can be added only for the destination address and not for the route pointing to destination a interface.**
vrf *vrf-name*	(Optional) Enter the keyword vrf followed by the name of the VRF to install IPv6 routes in that VRF.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Added support for VRF. Also included the `weight` parameter to support weighted ECMP feature. Introduced on the S6000-ON.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information

When the interface goes down, Dell Networking OS withdraws the route. The route is re-installed, by Dell Networking OS, when the interface comes back up. When a recursive resolution is "broken," Dell Networking OS withdraws the route. The route is re-installed, by Dell Networking OS, when the recursive resolution is satisfied.

After an IPv6 static route interface is created, if an IP address is not assigned to a peer interface, the peer must be manually pinged to resolve the neighbor information.

You can specify a weight for an IPv4 or IPv6 static route. If the weight value of a path is 0, then that path is not used for forwarding when weighted ECMP is in effect. Also, if a path corresponding to a static route (destination) has a non-zero weight assigned to it and other paths do not have any weight configured, then regular ECMP is used for forwarding.

You can specify the weight value only to destination address and not on the egress port.

A route is considered for weighted ECMP calculations only if each paths corresponding to that route is configured with a weight.

Example

```
Dell(conf)#ipv6 route 44::/64 33::1 weight 100
Dell(conf)#ipv6 route 44::/64 33::2 weight 200
Dell(conf)#do show running-config | grep ipv6 route
Dell(conf)#ipv6 route vrf vrf_test 44::/64 33::1 weight 100
Dell(conf)#ipv6 route vrf vrf_test 44::/64 33::2 weight 200
Dell(conf)#do show running-config | grep ipv6 route vrf
```

Related Commands

show ipv6 route — views the IPv6 configured routes.

ipv6 unicast-host-route

Enable the storage of extended IPv6 route prefixes (/65 to /128) in the L3 host table.

C9000 Series

Syntax

```
[no] ipv6 unicast-host-route
```

Defaults

Enabled; by default, extended IPv6 route prefixes are stored only in the L3 host table.

Command Modes

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.3(0.1)	Introduced on the S6000.

Usage Information

Use this command to enable programming of extended IPv6 (/65 to /128) route prefixes in the L3 host table. A warning message is displayed after you enter the command stating that this setting takes effect for existing routes only when IPv6 route prefixes are cleared from the LPM routing table (RTM). To enable storage of extended IPv6 route prefixes in the LPM table, disable this setting by entering the `no ipv6 unicast-host-route` command.

Example

```
Dell(conf)# ipv6 unicast-host-route
Warning: Command will take effect for existing routes only when IPv6
route prefixes are cleared from RTM
Dell(conf)#no ipv6 unicast-host-route
```

```
Warning: Command will take effect for existing routes only when IPv6
route prefixes are cleared from RTM
Dell(conf)#
```

ipv6 unicast-routing

Enable IPv6 Unicast routing.

C9000 Series

Syntax

`ipv6 unicast-routing`

To disable unicast routing, use the `no ipv6 unicast-routing` command.

Defaults

Enabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information

Because this command is enabled by default, it does not appear in the running configuration. When you disable unicast routing, the `no ipv6 unicast-routing` command is included in the running configuration. Whenever unicast routing is disabled or re-enabled, the system generates a syslog message indicating the action.

Disabling unicast routing on an E-Series chassis causes the following behavior:

- static and protocol learned routes are removed from RTM and from the CAM; packet forwarding to these routes is terminated
- connected routes and resolved neighbors remain in the CAM and new IPv6 neighbors are still discoverable
- additional protocol adjacencies (OSPFv3 and BGP4) are brought down and no new adjacencies are formed
- the IPv6 address family configuration (under router bgp) is deleted
- IPv6 Multicast traffic continues to flow unhindered

show cam-ipv6 extended-prefix

Display the currently configured and next-boot settings for extended IPv6 prefixes (/65 to /128) in LPM CAM.

C9000 Series

Syntax `show cam-ipv6 extended-prefix`

Defaults None

Command Modes EXEC

EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant Dell Networking OS Command Line Reference Guide.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.3(0.1)	Introduced on the S6000.

Usage Information You can use this command to view the maximum number of extended IPv6 prefix entries supported in LPM CAM. The output displays the current value and the new value applicable after a switch reload.

Example

```
Dell#show cam-ipv6 extended-prefix
Cam-Ipv6-LPM Extended Prefix
--------------------------------
Current Settings
cam-ipv6-max-/65-to-/128-Prefix : 2048
Dell(conf)#
```

show ipv6 cam linecard

Display the IPv6 CAM entries for the specified line card.

C9000 Series

Syntax `show ipv6 cam linecard` *`slot id`* `port-set` *`number`* `[vrf` *`vrf-name`*`][`*`X:X:X:X::X`* `| summary]`

Parameters

slot-id	Displays the cam entries for the mentioned linecard id.
port-set	Enter the keyword `port-set` and specify the port-set number. The port-set number value is 0.

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed and the name of the VRF to display IPv6 CAM entries corresponding to that VRF. **NOTE: If you do not specify this option, IPv6 CAM entries corresponding to the default VRF are displayed.**
X:X:X:X::X	(OPTIONAL) Enter the network address or host name.
summary	(OPTIONAL) Enter the keyword summary to display a table listing network prefixes and the total number prefixes which can be entered into the IPv6 CAM.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.1	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.

Example

```
Dell#show ipv6 cam linecard 10 port-set 0

Neighbor                    Mac-Addr          Port    VId  EC
-----------------------------------------------------------------
fe80::2ff:eff:fe3f:a1    00:00:00:00:00:00    CP      0    0
2::3                     00:00:00:00:00:00    CP      0    0

refix                    Mac-Addr           Port    VId  EC
-----------------------------------------------------------------
2::/64                   00:00:00:00:00:00   CP     0    0
fe80::/10                00:00:00:00:00:00   NuP    0    0
::/0                     00:00:00:00:00:00   CP     0
```

show ipv6 control-plane icmp

Displays the status of the icmp control-plane setting for the error eate limit setting.

C9000 Series

Syntax `show ipv6 control-plane icmp`

Default 100

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Example

show ipv6 fib linecard

Display all forwarding information base (FIB) entries for a line card.

C9000 Series

Syntax

```
show ipv6 fib linecard slot-id port-set number [vrf vrf-name] [summary | ipv6-address]
```

Parameters

slot-id	Enter the linecard *slot-id*. The range is from 0 to 11.
port-set *number*	Enter the keyword `port-set` and the port-set number value. The number value is 0.
vrf *vrf-name*	(Optional) Enter the keyword *vrf* followed by the name of the VRF to display neighbors corresponding to that VRF.
summary	(OPTIONAL) Enter the keyword `summary` to view a summary of entries in IPv6 cam.
ipv6-address	Enter the IPv6 address in the x:x:x:x::x/n format to display networks that have more specific prefixes. The range is from /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.

Example

```
Dell#show ipv6 fib linecard 10

Prefix                    Next-Hop     Mac-Addr           Port      VId  EC
-------------------------------------------------------------------------
::/0                       -           00:00:00:00:00:00  CP         0   0
2::/64                     ::, Te 10/1 00:00:00:00:00:00  CP         0   0
2::3/128                   ::1         00:00:00:00:00:00  CP         0   0
fe80::/10                  ::, Nu 0    00:00:00:00:00:00  BLK HOLE   0   0
fe80::2ff:eff:fe3f:a1/128 ::1          00:00:00:00:00:00  CP         0   0
```

show ipv6 flowlabel-zero

Display the flow label zero setting.

C9000 Series

Syntax `show ipv6 flowlabel-zero`

Default Disabled

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related Commands ipv6 nd dad attempts — Configure system to set the flow label field in the packets to zero.

show ipv6 interface

Display the status of interfaces configured for IPv6.

C9000 Series

Syntax

```
show ipv6 interface interface [linecard slot-id] [brief] [configured] [loopback interface-number] [managementethernet slot/port] [port-channel number] [tengigabitethernet slot | slot/port] [fortyGigE slot | slot/port] [tunnel tunnel-id] [vlan vlan-id]
```

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `Loopback` then a number from 0 to 16383. • For the Null interface, enter the keyword `null` then zero (0). • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a tunnel interface, enter the keyword `tunnel` then the tunnel ID. • For a VLAN interface, enter the keyword `VLAN`. • For a port channel interface, enter the keywords `port-channel`. • For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.
linecard *slot-id*	Enter the `linecard slot-id` parameters to specify the switch ports on a line card. The range of slot IDs is from 0 to 2.
brief	(OPTIONAL) View a summary of IPv6 interfaces.
configured	(OPTIONAL) View information on all IPv6 configured interfaces.
managementethernet *slot/ port*	(OPTIONAL) View information on an IPv6 Management port. Enter the slot number (0-1) and port number zero (0).
loopback	(OPTIONAL) View information for IPv6 Loopback interfaces.
port-channel	(OPTIONAL) View information for IPv6 port channels.
tengigabitethernet	(OPTIONAL) View information for an IPv6 tengigabitethernet interface.
fortyGigE	(OPTIONAL) View information for an IPv6 fortygigabitethernet interface.
tunnel *tunnel-id*	(OPTIONAL) View information for a tunnel interface.
vlan	(OPTIONAL) View information for IPv6 VLANs.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.11(0.0)	Updated the command output to include the unicast reverse path forwarding (uRPF) status.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for IPv6 recursive DNS addresses.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Added support for tunnel interface.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.4.2.1	Introduced on the S-Series.
8.2.1.0	Introduced on the E-Series ExaScale. Added support for the `managementethernet slot/port` parameter.
7.8.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information

The Management port is enabled by default (`no shutdown`). If necessary, use the `ipv6 address` command to assign an IPv6 address to the Management port.

Example

```
Dell# show ipv6 interface linecard 0
TenGigabitEthernet 0/2 is down, line protocol is down
  IPV6 is enabled
  Link Local address: fe80::7686:7aff:feff:6f08
  Global Unicast address(es):
    10:10:10:1::8, subnet is 10:10:10::/48 (MANUAL)
     Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:8
    ff02::1:ffff:6f08
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 27000 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements live for 1800 seconds
```

```
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64
  IPv6 unicast RPF check is not supported
```

```
Dell# show ipv6 interface linecard 0 configured
TenGigabitEthernet 0/2 is down, line protocol is down
  IPV6 is enabled
  Link Local address: fe80::7686:7aff:feff:6f08
  Global Unicast address(es):
    10:10:10:1::8, subnet is 10:10:10::/48 (MANUAL)
     Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:8
    ff02::1:ffff:6f08
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 27000 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements live for 1800 seconds
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64
  IPv6 unicast RPF check is not supported
```

```
Dell# show ipv6 interface linecard 0 configured
TenGigabitEthernet 0/2 is down, line protocol is down
  IPV6 is enabled
  Link Local address: fe80::7686:7aff:feff:6f08
  Global Unicast address(es):
    10:10:10:1::8, subnet is 10:10:10::/48 (MANUAL)
     Remaining lifetime: infinite
  Global Anycast address(es):
  Joined Group address(es):
    ff02::1
    ff02::2
    ff02::1:ff00:8
    ff02::1:ffff:6f08
  ND MTU is 0
  ICMP redirects are not sent
  DAD is enabled, number of DAD attempts: 3
  ND reachable time is 27000 milliseconds
  ND base reachable time is 30000 milliseconds
  ND advertised reachable time is 0 milliseconds
  ND advertised retransmit interval is 0 milliseconds
  ND router advertisements are sent every 200 to 600 seconds
  ND router advertisements live for 1800 seconds
  ND advertised hop limit is 64
  IPv6 hop limit for originated packets is 64
  IPv6 unicast RPF check is not supported
```

```
Dell# show ipv6 interface linecard 1 configured | grep ff02
    ff02::1
    ff02::2
    ff02::1:ff00:6
    ff02::1:ffff:6f08
    ff02::1
    ff02::2
    ff02::1:ff00:4
    ff02::1:ffff:6f08
```

show ipv6 mld_host

Display the IPv6 MLD host counters.

C9000 Series

Syntax `show ipv6 mld_host`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Neworking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information The following describes the `show ipv6 mld-host` command shown in the following example.

Field	Description
Valid MLD Packets	The total number of packets received and sent from the last time the elapsed time was cleared.
Reports	The total number of reports (queries and unsolicited reports generated from joins or leaves) that have been received or sent.
Leaves	The number of Multicast leaves that have been sent.
MLDv1 queries	The number of MLDv1 queries that have been received.
MLDv2 queries	The number of MLDv2 queries that have been received.
Malformed Packets	The number of MLDv1 and MLDv2 packets that do not match the requirement for a valid MLD packet.

Example

```
MLD Host Traffic Counters
Elapsed time since counters cleared: 0028:33:52
                    Received   Sent
Valid MLD Packets   97962      18036
Reports             79962      18034
Leaves              ----       0
MLDv2 Queries       18000      ----
MLDv1 Queries       0          ----
Errors:
Malformed Packets: 4510
```

show ipv6 neighbors

Display information about the IPv6 neighbors discovered on the switch CPUs.

C9000 Series

Syntax

```
show ipv6 neighbors [cpu rp] [ipv6-address] {ipv6-address}] [interface
interface [vrf vrf-name]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to display the neighbors corresponding to that VRF. **NOTE: If you do not specify this option, neighbors corresponding to the default VRF are displayed.**
cpu rp	Enter the keywords `cpu rp` to display information about IPv6 neighbors learned only on the Route Processor.
ipv6–address	Enter the IPv6 address of a neighbor to display information about the specified device.
ipv6-address	Enter the IPv6 address of the neighbor in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zero.**
interface *interface*	Enter the keyword `interface` then the interface type and slot/port or number information:

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000–ON.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

Usage Information

When you issue the `show ipv6 neighbors` without specifying any options, it will display all IPv6 neighbor addresses stored on the control processor (CP).

Example

```
Dell#show ipv6 neighbors

*    - Active session role
Ad Dn - Admin Down
B    - BGP
C    - CLI
I    - ISIS
O    - OSPF
R    - Static Route (RTM)

  LocalAddr  RemoteAddr  Interface State Rx-int Tx-int Mult Clients
* 10.1.3.2   10.1.3.1    Te 1/3    Up    300    250    3    C
```

```
Dell#show ipv6 neighbors detail

Session Discriminator: 1
Neighbor Discriminator: 1
Local Addr: 10.1.3.2
Local MAC Addr: 00:01:e8:02:15:0e
Remote Addr: 10.1.3.1
Remote MAC Addr: 00:01:e8:27:2b:f1
Int: TenGigabitEthernet 1/3
State: Up
Configured parameters:
 TX: 100ms, RX: 100ms, Multiplier: 3
Neighbor parameters:
 TX: 250ms, RX: 300ms, Multiplier: 4
Actual parameters:
 TX: 300ms, RX: 250ms, Multiplier: 3
Role: Active
Delete session on Down: False
Client Registered: CLI
Uptime: 00:02:04
Statistics:
 Number of packets received from neighbor: 376
 Number of packets sent to neighbor: 314
 Number of state changes: 2
 Number of messages from IFA about port state change: 0
 Number of messages communicated b/w Manager and Agent: 6
Dell#
```

show ipv6 route

Displays the IPv6 routes.

C9000 Series

Syntax

```
show ipv6 route [ipv6-address prefix-length] [hostname] [all] [bgp as number]
[connected] [isis tag] [list prefix-list name] [ospf process-id][vrf vrf-name]
[rip] [static] [summary]
```

Parameters

ipv6-address prefix-length (OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

hostname	(OPTIONAL) View information for this IPv6 routes with Host Name.
all	(OPTIONAL) View information for all IPv6 routes.
bgp	(OPTIONAL) View information for all IPv6 BGP routes.
connected	(OPTIONAL) View only the directly connected IPv6 routes.
isis	(OPTIONAL) View information for all IPv6 IS-IS routes.
list	(OPTIONAL) View the IPv6 prefix list.
ospf	(OPTIONAL) View information for all IPv6 OSPF routes.
vrf *vrf-name*	(Optional) Enter the keyword vrf and the name of the VRF to display IPv6 routes corresponding to that VRF. **NOTE: If you do not specify this option, routes corresponding to the default VRF are displayed.**
rip	(OPTIONAL for E-Series only) View information for all IPv6 RIP routes.
static	(OPTIONAL) View only routes configured by the `ipv6 route` command.
summary	(OPTIONAL) View a brief list of the configured IPv6 routes.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on S6000–ON
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

Usage Information

The following describes the `show ipv6 route` command shown in the following examples.

Field	Description
(undefined)	Identifies the type of route:

Field	Description
	• L = Local • C = connected • S = static • R = RIP • B = BGP • IN = internal BGP • EX = external BGP • LO = Locally Originated • O = OSPF • IA = OSPF inter-area • N1 = OSPF NSSA external type 1 • N2 = OSPF NSSA external type 2 • E1 = OSPF external type 1 • E2 = OSPF external type 2 • i = IS-IS • L1 = IS-IS level-1 • L2 = IS-IS level-2 • IA = IS-IS inter-area • * = candidate default • > = non-active route • + = summary routes
Destination	Identifies the route's destination IPv6 address.
Gateway	Identifies whether the route is directly connected and on which interface the route is configured.
Dist/Metric	Identifies if the route has a specified distance or metric.
Last Change	Identifies when the route was last changed or configured.

Example

```
Dell#show ipv6 route

Codes: C - connected, L - local, S - static, R - RIP,
       B - BGP, IN - internal BGP, EX - external BGP,LO - Locally Originated,
       O - OSPF, IA - OSPF inter area, N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2, E1 - OSPF external type 1,
       E2 - OSPF external type 2, i - IS-IS, L1 - IS-IS level-1,
       L2 - IS-IS level-2, IA - IS-IS inter area, * - candidate default,
Gateway of last resort is not set

       Destination  Dist/Metric,      Gateway,   Last Change
       ------------------------------------------------------
  C    2::/64 [0/0]
          Direct, Te 10/1, 00:01:53
  L    fe80::/10 [0/0]
          Direct, Nu 0, 00:01:53
```

Example (Summary)

```
Dell#show ipv6 route summary

Route Source  Active Routes  Non-active Routes
connected     5              0
static        0              0
```

```
Total          5               0
Total 5 active route(s) using 952 bytes
```

29

iSCSI Optimization

Internet small computer system interface (iSCSI) optimization enables quality-of-service (QoS) treatment for iSCSI storage traffic on a switch.

To configure and verify the iSCSI optimization feature, use the following Dell Networking OS commands.

Topics:

- advertise dcbx-app-tlv
- iscsi aging time
- iscsi cos
- iscsi enable
- iscsi priority-bits
- iscsi profile-compellant
- iscsi target port
- show iscsi
- show iscsi session
- show iscsi session detailed
- show run iscsi

advertise dcbx-app-tlv

Configure DCBX to send iSCSI TLV advertisements.

C9000 Series

Syntax

```
advertise dcbx-app-tlv iscsi
```

To disable DCBX iSCSI TLV advertisements, use the `no advertise dcbx-app-tlv iscsi` command.

Defaults

Disabled.

Command Modes

PROTOCOL LLDP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the Z9500.

Usage Information

You can configure iSCSI TLVs to send either globally or on a specified interface. The interface configuration takes priority over global configuration.

NOTE: The `advertise dcbx-app-tlv iscsi` command is not supported on cascade interfaces or extended ports.

iscsi aging time

Set the aging time for iSCSI sessions.

C9000 Series

Syntax

`iscsi aging time` *time*

To remove the iSCSI session aging time, use the `no iscsi aging time` command.

Parameters

time	Enter the aging time for the iSCSI session. The range is from 5 to 43,200 minutes.

Defaults

10 minutes

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the Z9500.

iscsi cos

Set the QoS policy that is applied to the iSCSI flows.

C9000 Series

Syntax

`iscsi cos {enable | disable | dot1p` *vlan-priority-value* `[remark] | dscp` *dscp-value* `[remark]}`

To disable the QoS policy, use the `no iscsi cos` command.

Parameters

enable	Enter the keyword `enable` to allow the application of preferential QoS treatment to iSCSI traffic so that the iSCSI packets are scheduled in the switch with a dot1p priority 4 regardless of the VLAN priority tag in the packet. The default is: the iSCSI packets are handled with dotp1 priority 4 without remark.
disable	Enter the keyword `disable` to disable the application of preferential QoS treatment to iSCSI frames.

	dot1p *vlan-priority-value*	Enter the dot1p value of the VLAN priority tag assigned to the incoming packets in an iSCSI session. The range is from 0 to 7. The default is the dot1p value in ingress iSCSI frames is not changed and is the same priority is used in iSCSI TLV advertisements if you did not enter the `iscsi priority-bits` command.
	dscp *dscp-value*	Enter the DSCP value assigned to the incoming packets in an iSCSI session. The valid range is from 0 to 63. The default is: the DSCP value in ingress packets is not changed.
	remark	Marks the incoming iSCSI packets with the configured dot1p or DSCP value when they egress to the switch. The default is: the dot1and DSCP values in egress packets are not changed.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the Z9500.

Usage Information By default, iSCSI flows are assigned to dot1p priority 4.

iscsi enable

Globally enable iSCSI optimization.

C9000 Series

Syntax `iscsi enable`

To disable iSCSI optimization, use the `no iscsi enable` command.

Parameters

enable	Enter the keyword `enable` to enable the iSCSI optimization feature.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.6(0.0)	Introduced on the Z9500.

iscsi priority-bits

Configure the priority bitmap that advertises in the iSCSI application TLVs.

C9000 Series

Syntax `iscsi priority-bits`

To remove the configured priority bitmap, use the `no iscsi priority-bits` command.

Defaults **4** (0x10 in the bitmap)

Command Modes PROTOCOL LLDP (only on the global, not on the interface)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the Z9500.

iscsi profile-compellant

Configure the auto-detection of Dell Compellent arrays on a port.

C9000 Series

Syntax `iscsi profile-compellent`

Defaults Dell Compellent disk arrays are not detected.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6.(0.0)	Introduced on the Z9500.

iscsi target port

Configure the iSCSI target ports and optionally, the IP addresses on which iSCSI communication is monitored.

C9000 Series

Syntax

`iscsi target port [tcp-port-2...tcp-port-16]ip-address [ip-address]`

To remove the configured iSCSI target ports or IP addresses, use the `no iscsi target port` command.

Parameters

tcp-port-2...tcpport- 16	Enter the tcp-port number of the iSCSI target ports. The `tcp-port-n` is the TCP port number or a list of TCP port numbers on which the iSCSI target listens to requests. Separate port numbers with a comma. The default is **860, 3260**.
ip-address (Optional)	Enter the ip-address that the iSCSI monitors. The ip-address specifies the IP address of the iSCSI target.

Defaults

860, 3260

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the Z9500.

Usage Information

You can configure up to 16 target TCP ports on the switch in one command or multiple commands.

When you use the `no iscsi target port` command and the TCP port you want to delete is one bound to a specific IP address, the IP address value must be included in the command.

show iscsi

Display the currently configured iSCSI settings.

C9000 Series

Syntax

`show iscsi`

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the Z9500.

Example

```
Dell#show iscsi
iSCSI is enabled
iSCSI session monitoring is disabled
iSCSI COS : dot1p is 4 no-remark
Session aging time: 10
Maximum number of connections is 256
------------------------------------------------
iSCSI Targets and TCP Ports:
------------------------------------------------
TCP Port Target IP Address
3260
860
```

Related Commands

- show iscsi session— displays information about active iSCSI sessions on the switch.
- show iscsi session detailed— displays detailed information about active iSCSI sessions on the switch.
- show run iscsi— shows `run iscsi`.

show iscsi session

Display information about active iSCSI sessions on the switch.

C9000 Series

Syntax

```
show iscsi session
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the Z9500.

Example

```
Dell# show isci session
Session 0:
------------------------------------------------------
```

```
Target: iqn.2001-05.com.equallogic:0-8a0906-0e70c2002-10a0018426a48c94-iom010
Initiator: iqn.1991-05.com.microsoft:win-x9l8v27yajg
ISID: 400001370000

Session 1:
-------------------------------------------------------
Target: iqn.2001-05.com.equallogic:0-8a0906-0f60c2002-0360018428d48c94-iom011
Initiator: iqn.1991-05.com.microsoft:win-x9l8v27yajg
ISID: 400001370000.
```

Usage Information

The switch learns only the active sessions which it observes; sessions flowing through an adjacent switch are not learned.

After you reload the switch, session information exchanged during the initial handshake is not available. If the switch picks up session communication after reloading, it detects iSCSI sessions in progress but sometimes cannot obtain complete session information. Incomplete information about active iSCSI sessions is not displayed in `show iscsi session` command output.

In a VLT configuration, `show iscsi session` output is not accurate unless there are iSCSI traffic flows on VLT LAGs on both the target and the initiator side of the VLT domain.

Related Commands

- show iscsi — displays the currently configured iSCSI settings.
- show iscsi session detailed— displays detailed information about active iSCSI sessions on the switch.
- show run iscsi— shows `run iscsi`.

show iscsi session detailed

Display detailed information on active iSCSI sessions on the switch.

C9000 Series

Syntax

```
show iscsi session detailed [session isid]
```

Parameters

isid	Enter the session's iSCSi ID to display detailed information about the specified iSCSi session.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the Z9500.

Example

```
Dell# show isci session detailed
Session 0 :
-------------------------------------------------
Target:iqn.2010-11.com.ixia:ixload:iscsi-TG1
Initiator:iqn.2010-11.com.ixia.ixload:initiator-iscsi-2c
Up Time:00:00:01:28(DD:HH:MM:SS)
Time for aging out:00:00:09:34(DD:HH:MM:SS)
ISID:806978696102
Initiator  Initiator Target      Target  Connection
IP Address TCP Port  IP Address  TCPPort ID
10.10.0.44 33345     10.10.0.101 3260    0
Session 1 :
-------------------------------------------------
Target:iqn.2010-11.com.ixia:ixload:iscsi-TG1
Initiator:iqn.2010-11.com.ixia.ixload:initiator-iscsi-35
Up Time:00:00:01:22(DD:HH:MM:SS)
Time for aging out:00:00:09:31(DD:HH:MM:SS)
ISID:806978696102
Initiator  Initiator Target     Target  Connection
IP Address TCP Port  IP Address TCPPort ID
10.10.0.53 33432     10.10.0.101 3260   0
```

Related Commands

- show iscsi— displays the currently configured iSCSI settings.
- show iscsi session— displays information about active iSCSI sessions on the switch.
- show run iscsi — shows `run iscsi`.

show run iscsi

Display all globally configured non-default iSCSI settings in the current Dell Networking OS session.

C9000 Series

Syntax `show run iscsi`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the Z9500.

Related Commands

- show iscsi— displays the currently configured iSCSI settings.
- show iscsi session— displays detailed information about active iSCSI sessions on the switch.
- show iscsi session detailed— displays detailed information on active iSCSI sessions on the switch.

30

Layer 2

This chapter describes commands to configure Layer 2 features.

This chapter contains the following sections:

- MAC Addressing Commands
- Virtual LAN (VLAN) Commands
- Far-End Failure Detection (FEFD)

Topics:

- MAC Addressing Commands
- Virtual LAN (VLAN) Commands
- Far-End Failure Detection (FEFD)

MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses.

clear mac-address-table

Clear the MAC address table of all MAC address learned dynamically.

C9000 Series

Syntax

```
clear mac-address-table {dynamic | sticky }{address mac-address | all |
interface interface | vlan vlan-id}
```

Parameters

dynamic	Enter the keyword `dynamic` to specify dynamically-learned MAC addresses.
sticky	Enter the keyword `sticky` to specify sticky MAC addresses.
address *mac-address*	Enter the keyword `address` then a MAC address in nn:nn:nn:nn:nn:nn format.
all	Enter the keyword `all` to delete all MAC address entries in the MAC address table.
interface *interface*	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

vlan *vlan-id* Enter the keyword `vlan` then a VLAN ID number from 1 to 4094.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Added support for sticky MAC addresses.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

mac-address-table aging-time

Specify an aging time for MAC addresses to remove from the MAC address table.

C9000 Series

Syntax `mac-address-table aging-time` *seconds*

Parameters

seconds Enter either zero (0) or a number as the number of seconds before MAC addresses are relearned. To disable aging of the MAC address table, enter `0`. The range is from 10 to 1000000. The default is **1800 seconds**.

Defaults **1800 seconds**

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	On the E-Series, available in INTERFACE VLAN context, reduced the minimum aging time in the INTERFACE VLAN context from 10 seconds to 1 second.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

mac learning-limit — sets the MAC address learning limits for a selected interface.

show mac-address-table aging-time — displays the MAC aging time.

mac-address-table disable-learning

Disable MAC address learning from LACP or LLDP BPDUs.

Syntax

```
mac-address-table disable-learning [lacp | lldp]
```

Parameters

lacp	Enter `lacp` to disable MAC address learning from LACP BPDUs.
lldp	Enter `LLDP` to disable MAC address learning from LLDP BPDUs.

Defaults

Disabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.0)	Introduced on the S3048–ON, S3100 series, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, Z9100–ON, and Z9500.

Usage Information

If you use the `mac-address-table disable-learning` command without specifying any option, the system does not learn source MAC addresses from LACP or LLDP BPDUs.

mac-address-table static

Associate specific MAC or hardware addresses to an interface and VLANs.

C9000 Series

Syntax

`mac-address-table static` *`mac-address`* `{multicast vlan` *`vlan-id`* `output—range` *`interface`*`}{`*`output interface`* `vlan` *`vlan-id`*`}`

To remove a MAC address, use the `no mac-address-table static` *`mac-address`* `output` *`interface`* `vlan` *`vlan-id`* command.

Parameters

mac-address	Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
multicast	Enter a vlan port to where L2 multicast MAC traffic is forwarded. **NOTE: Use this option if you want multicast functionality in an L2 VLAN without IGMP protocols.**
output *interface*	For a unicast MAC address, enter the keyword `output` then one of the following interfaces for which traffic is forwarded: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
output-range *interface*	For a multicast MAC address, enter the keyword `output-range` then one of the following interfaces to indicate a range of ports for which traffic is forwarded: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
vlan *vlan-id*	Enter the keyword `vlan` then a VLAN ID number from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for output range parameter for S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example (Unicast)

```
mac-address-table static 00:01:00:00:00:01 {output Te 0/2 vlan 2}
```

Example (Multicast)

```
mac-address-table static 01:00:5E:01:00:01 {multicast vlan 2 output—range Te 0/2,Te 0/3}
```

Related Commands

show mac-address-table — displays the MAC address table.

mac-address-table station-move refresh-arp

Ensure that address resolution protocol (ARP) refreshes the egress interface when a station move occurs due to a topology change.

C9000 Series

Syntax

```
[no] mac-address-table station-move refresh-arp
```

Defaults

Enabled.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

For details about using this command, see the "NIC Teaming" section of the Layer 2 chapter in the *Dell Networking OS Configuration Guide*.

To disable the ARP refresh feature, use the `no mac-address-table station-move refresh-arp` command.

Use this command in Configuration Terminal Batch mode to refresh the egress interface in a dual-homing setup.

mac-address-table station-move threshold

Specify the threshold and time interval for the maximum number of station moves on PE ports. When the number of station moves for a specified MAC address exceeds the configured threshold in the configured time, a loop is detected on PE ports. The loop is prevented by bringing down the line protocol on all active ports in the learned path, except for the port with the lowest interface index (ifIndex).

C9000 Series

Syntax

`[no] mac-address-table station-move threshold` *`number`* `interval` *`seconds`*

Parameters

threshold *number*	Enter the keyword `threshold` with the maximum number of times a MAC-address station move is detected within the configured interval. The range is from 5 to 50.
interval *seconds*	Enter the keyword `interval` with the interval (in seconds). The range is from 1 to 60.

Defaults

Not configured.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C1048P.

Usage Information

As xSTP protocols are not supported on PEs, use this command to detect possible loops on PE ports.

Use this command in Configuration Terminal Batch mode to detect the possible loops in a dual-homing setup.

If a station move for a MAC address is detected above the configured threshold and within the specified time, a syslog message is triggered with the port information. All ports on which the station move was detected are shut down, except for the port with the lowest interface index. Only the port with the lowest ifIndex remains active. For example:

```
Jun 18 09:55:35: %RPM0-P:RP %MACMGR-1-PE LOOP DETECTION: Loop occurred on PE
interfaces:oldInterface: peGigE 0/2/47, newInterface: peGigE 0/1/20,vlanId:
3902, macAddr: 00:aa:00:00:00:
```

To display the PE ports that are shut down due to loop detection, enter the `show mac learning-limit violate-action` command.

```
Dell# show mac learning-limit violate-action
Interface      Violation-Type Violate-Action Status
PeGi 0/2/47    Pe-Loop        Shutdown       PEloop-disable
PeGi 100/0/20  Pe-Loop        Shutdown       PEloop-disable
PeGi 255/0/47  Pe-Loop        Shutdown       PEloop-disable
Po 1           Pe-Loop        Shutdown       PEloop-disable
Po 100         Pe-Loop        Shutdown       PEloop-disable
```

To display the reason why the line protocol is down on a PE port or port channel, enter the `show interface` command.

```
Dell(conf-if-po-1)#do show interface port-channel 1
Port-channel 1 is up, line protocol is down(Pe Loop Detection)
```

When a PE interface is shut down due to a PE loop violation, you must manually reset it. To reset the interface, shut it down by entering the `shutdown` command and then re-enable it by entering the `no shutdown` command.

mac learning-limit

Limit the maximum number of MAC addresses (static + dynamic) learned on a selected interface.

C9000 Series

Syntax

```
mac learning-limit address_limit [vlan vlan-id] [station-move-violation
[dynamic]] [dynamic [no-station-move| station-move]]
```

Parameters

address_limit	Enter the maximum number of MAC addresses that can be learned on the interface. The range is from 1 to 1000000.
vlan *vlan-id*	E-Series only: Enter the keyword then the VLAN ID. The range is from 1 to 4094.
dynamic	(OPTIONAL) Enter the keyword `dynamic` to allow aging of MACs even though a learning limit is configured.
station-move-violation	(OPTIONAL) Enter the keywords `station-move` to allow a station move on learned MAC addresses.

Defaults

- On S-Series, the default behavior is dynamic.

NOTE: "Static" means manually entered addresses, which do not age.

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Deprecated the `no-station-move` command (replaced by the `mac-learning-limit mac-address-sticky` command).
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the `vlan` option on the E-Series.
8.2.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series. Added the `station-move` option.
6.5.1.0	Added support for MAC Learning-Limit on the LAG.

Usage Information

This command and its options are supported on physical interfaces, static LAGs, LACP LAGs, and VLANs.

If you do not specify the `vlan` option, the MAC address counters are not VLAN-based. That is, the sum of the addresses learned on all VLANs (not having any learning limit configuration) is counted against the MAC learning limit.

MAC Learning Limit violation logs and actions are not available on a per-VLAN basis.

With the keyword `no-station-move` option, MAC addresses learned through this feature on the selected interface persist on a per-VLAN basis, even if received on another interface. Enabling or disabling this option has no effect on already learned MAC addresses.

After the MAC address learning limit is reached, the MAC addresses do not age out unless you add the `dynamic` option. To clear statistics on MAC address learning, use the `clear counters` command with the learning-limit parameter.

NOTE: If you configure this command on an interface in a routed VLAN, and after the MAC addresses learned reaches the limit set in the `mac learning-limit` command, IP protocols are affected. For example, VRRP sets multiple VRRP Masters and OSPF may not come up.

When a channel member is added to a port-channel and there is not enough ACL CAM space, the MAC limit functionality on that port-channel is undefined. When this occurs, un-configure the existing configuration first and then reapply the limit with a lower value.

Related Commands

- clear counters — Clear counters used in the `show interface` command.
- clear mac-address-table — clears the MAC address table of all MAC address learned dynamically.
- mac learning-limit mac-address-sticky — Replaces deprecated `no-station-move` parameter.
- show mac learning-limit — displays MAC learning-limit configuration.

mac learning-limit learn-limit-violation

Configure an action for a MAC address learning-limit violation.

C9000 Series

Syntax

```
mac learning-limit learn-limit-violation {log | shutdown}
```

To return to the default, use the `no mac learning-limit learn-limit-violation {log | shutdown}` command.

Parameters

log	Enter the keyword `log` to generate a syslog message on a learning-limit violation.
shutdown	Enter the keyword `shutdown` to shut down the port on a learning-limit violation.

Defaults none

Command Modes INTERFACE (conf-if-interface-slot/port)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

Usage Information This command is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands show mac learning-limit — displays details of the mac learning-limit.

mac learning-limit mac-address-sticky

Maintain the dynamically learned mac addresses as sticky MAC addresses on the selected port.

C9000 Series

Syntax

```
mac learning-limit mac-address-sticky
```

To convert the sticky MAC addresses to dynamic MAC addresses, use the `no mac learning-limit` command.

Parameters

mac-address-sticky	Configures the dynamic MAC addresses as sticky on an interface.

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Usage Information If you configure `mac-learn-limit` and the sticky MAC feature is enabled, dynamically learned MAC addresses are converted to sticky for that port. Any new MAC address that is learned also becomes sticky for that port.

Related Commands show mac learning-limit — displays the details of the mac learning-limit.

mac learning-limit station-move-violation

Specify the actions for a station move violation.

C9000 Series

Syntax `mac learning-limit station-move-violation {log | shutdown-both | shutdown-offending | shutdown-original}`

To disable a configuration, use the `no mac learning-limit station-move-violation` command, then the configured keyword.

Parameters

log	Enter the keyword `log` to generate a syslog message on a station move violation.
shutdown-both	Enter the keyword `shutdown` to shut down both the original and offending interface and generate a syslog message.
shutdown-offending	Enter the keywords `shutdown-offending` to shut down the offending interface and generate a syslog message.
shutdown-original	Enter the keywords `shutdown-original` to shut down the original interface and generate a syslog message.

Defaults none

Command Modes INTERFACE (conf-if-interface-slot/port)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the S-Series.
7.8.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

Usage Information This command is supported on physical interfaces, static LAGs, and LACP LAGs.

Related Commands show mac learning-limit — displays details of the mac learning-limit.

mac learning-limit reset

Reset the MAC address learning-limit error-disabled state.

C9000 Series

Syntax `mac learning-limit reset`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.2.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

mac port-security

Enable or disable the port security feature globally in the system.

Syntax

```
mac port-security
```

To disable the port security, use the `no mac port-security` command.

Defaults

Enabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.0)	Introduced on the C9010, MXL, FN IOM, S3100 series, S4810, S4820T, S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, and Z9500.

Usage Information

Only if you enable the port security, you will be able to configure MAC address learning limit configurations on the interface level.

When you disable the port security, all the interface level configurations are reset. Also, all dynamically learnt MAC addresses on the interfaces configured with MAC address learning limit are cleared.

show cam mac linecard (dynamic or static)

Display the CAM size and the portions allocated for MAC addresses and for MAC ACLs.

C9000 Series

Syntax

```
show cam mac linecard slot-id port-set port-pipe [address mac_addr | dynamic |
interface interface | static | vlan vlan-id]
```

Parameters

linecard *slot-id*	(REQUIRED) Enter the keyword `linecard` then a slot number to select the linecard for which to gather information. The range of C9000 slot IDs are from 0 to 11.
port-set *port-pipe*	(REQUIRED) Enter the keywords `port-set` then a port-pipe number to specify the port pipe for which to gather information. The range of port pipe numbers is from 0 to 0.
address *mac-addr*	(OPTIONAL) Enter the keyword `address` then a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.

dynamic	(OPTIONAL) Enter the keyword `dynamic` to display only those MAC addresses the switch dynamically learns.
interface *interface*	(OPTIONAL) Enter the keyword `interface` then the interface type, slot and port information: • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.
static	(OPTIONAL) Enter the keyword `static` to display only those MAC addresses specifically configured on the switch.
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell# show cam mac linecard 1 port-set 0
PVlanId     Mac Address      Region    Interface
 1      00:01:02:03:04:09   DYNAMIC     Fo 2/0
 0      74:86:7a:ff:6f:1c   LOCAL_DA    00001
 1      00:11:22:33:44:55   STATIC      Fo 2/8
 1      00:01:02:03:04:07   DYNAMIC     Fo 2/0
 1      00:01:02:03:04:08   DYNAMIC     Fo 2/0
 0      ff:ff:ff:ff:ff:ff   STATIC      00001
```

```
1       00:01:02:03:04:05   DYNAMIC     Fo 2/0
1       00:01:02:03:04:06   DYNAMIC     Fo 2/0
```

show mac-address-table

Display the MAC address table.

C9000 Series

Syntax

```
show mac-address-table [address mac-address | interface interface | vlan vlan-id] [aging-time] [dynamic | static] [count [vlan vlan-id] [interface interface-type [slot [/port]]]]
```

Parameters

address *mac-address*	(OPTIONAL) Enter the keyword `address` then a MAC address in the nn:nn:nn:nn:nn:nn format to display information on that MAC address.
dynamic	(OPTIONAL) Enter the keyword `dynamic` to display only those MAC addresses the switch dynamically learns. Optionally, you can also add one of these combinations: `address`/*`mac-address`*, `interface`/*`interface`*, or `vlan` *`vlan-id`*.
static	(OPTIONAL) Enter the keyword `static` to display only those MAC addresses specifically configured on the switch. Optionally, you can also add one of these combinations: `address`/*`mac-address`*, `interface`/*`interface`*, or `vlan` *`vlan-id`*.
aging-time	Enter the keyword `aging-time` to display only aging-time information.
interface *interface*	(OPTIONAL) Enter the keyword `interface` then the interface type, slot and port information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.
interface *interface-type*	(OPTIONAL) Instead of entering the keyword `interface` then the interface type, slot and port information, as above, you can enter the interface type, then just a slot number.
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.
count	(OPTIONAL) Enter the keyword `count`, then optionally, by an interface or VLAN ID, to display total or interface-specific static addresses, dynamic addresses, and MAC addresses in use.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Updated the output.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show mac-address-table` command shown in the following example.

Column Heading	Description
VlanId	Displays the VLAN ID number.
Mac Address	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
Type	Lists whether the MAC address was manually configured (Static), learned dynamically (Dynamic), or associated with a specific port (Sticky).
Interface	Displays the interface type and slot/port information. The following abbreviations describe the interface types: • po — Port Channel then a number. The range is from 1 to 255 for TeraScale. • te — 10-Gigabit Ethernet then a slot/port. • fo — 40-Gigabit Ethernet then a slot/port.
State	Lists if the MAC address is in use (Active) or not in use (Inactive).

Example

```
Dell(conf)#do show mac-address-table
Codes: *N - VLT Peer Synced MAC
VlanId    Mac Address          Type          Interface       State
2     00:00:00:00:00:01      Dynamic (N)    Po 128         Active
2     00:00:00:00:00:02      Dynamic (N)    Po 10           Active
2     00:00:00:00:00:03      Dynamic            Po 100         Active
2     00:00:00:00:00:04      Dynamic            Po 10           Active
```

Usage Information

The following describes the `show mac-address-table` command shown in the following example.

Column Heading	Description
VlanId	Displays the VLAN ID number.
Mac Address	Displays the MAC address in nn:nn:nn:nn:nn:nn format.
Type	Lists whether the MAC address was manually configured (Static), learned (Dynamic), or associated with a specific port (Sticky). An (N) indicates that the specified MAC address has been learnt by a neighbor and is synced to the node.
Interface	Displays the interface type and slot/port information. The following abbreviations describe the interface types: • po — Port Channel followed by a number. Range for Terascale is from 1 to 255. \ • te — 10–Gigabit Ethernet followed by a slot/port. • fo — 40-Gigabit Ethernet then a slot/port.
State	Lists if the MAC address is in use (Active) or not in use (Inactive).

The following describes the `show mac-address-table count` command shown in the following example.

Line Beginning With	Description
MAC Entries...	Displays the number of MAC entries learned per VLAN.
Dynamic Address...	Lists the number of dynamically learned MAC addresses.
Static Address...	Lists the number of user-defined MAC addresses.
Total MAC...	Lists the total number of MAC addresses the switch uses.

Example (Count)

```
Dell# show mac-address-table count
MAC Entries for all vlans :
Dynamic Address Count :                110
Static Address (User-defined) Count : 0
Sticky Address Count :                 0
Total Synced Mac from Peer(N):         100
Total MAC Addresses in Use:            110
Dell#
```

Related Commands show mac-address-table aging-time — displays MAC aging time.

show mac-address-table aging-time

Display the aging times assigned to the MAC addresses on the switch.

C9000 Series

Syntax `show mac-address-table aging-time [vlan vlan-id]`

Parameters

vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display the MAC address assigned to the VLAN. The range is from 1 to 4094.

Command Modes

- EXEC

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the `vlan` option on the E-Series.
7.7.1.0	Introduced on the C-Series and S-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell#show mac-address-table aging-time
  Mac-address-table aging time : 1800

Dell#
```

Related Commands

show mac-address-table — displays the current MAC address configuration.

show mac learning-limit

Display MAC address learning limits set for various interfaces.

C9000 Series

Syntax

```
show mac learning-limit [violate-action] [detail] [interface interface]
```

Parameters

violate-action	(OPTIONAL) Enter the keywords `violate-action` to display the MAC learning limit violation status.
detail	(OPTIONAL) Enter the keyword `detail` to display the MAC learning limit in detail.
interface *interface*	(OPTIONAL) Enter the keyword `interface` with the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the `vlan` option on the E-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Added support for the `violate-action` and `detail` options.
6.5.1.0	Added support for Port Channel.

Example

```
Dell#show mac learning-limit
Interface  Learning  Dynamic    Static     Unknown SA
Slot/port  Limit     MAC count  MAC count  Drops
Te 1/0     10        0          0          0
Te 1/1     5         0          0          0

Dell#show mac learning-limit interface gigabitethernet 1/0
Interface  Learning  Dynamic    Static     Unknown SA
Slot/port  Limit     MAC count  MAC count  Drops
Te 1/0     10        0          0          0
```

Virtual LAN (VLAN) Commands

The following commands configure and monitor virtual LANs (VLANs). VLANs are a virtual interface and use many of the same commands as physical interfaces.

You can configure an IP address and Layer 3 protocols on a VLAN called Inter-VLAN routing. FTP, TFTP, ACLs and SNMP are not supported on a VLAN.

Occasionally, while sending broadcast traffic over multiple Layer 3 VLANs, the VRRP state of a VLAN interface may continually switch between Master and Backup.

NOTE: For more information, refer to VLAN Stacking and VLAN-related commands, such as portmode hybrid in the Interfaces chapter.

default vlan-id

Specify a VLAN as the Default VLAN.

C9000 Series

Syntax

`default vlan-id vlan-id`

To remove the default VLAN status from a VLAN and VLAN 1 does not exist, use the `no default vlan-id vlan-id` syntax.

Parameters

vlan-id	Enter the VLAN ID number of the VLAN to become the new Default VLAN. The range is from 1 to 4094. The default is **1**.

Defaults

The Default VLAN is VLAN **1**.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

To return VLAN 1 as the Default VLAN, use this command syntax (`default-vlan-id 1`).

The Default VLAN contains only untagged interfaces.

Use this command in Configuration Terminal Batch mode to specify a default VLAN in a dual-homing setup.

Related Commands interface vlan — configures a VLAN.

default-vlan disable

Disable the default VLAN so that all switchports are placed in the Null VLAN until they are explicitly configured as a member of another VLAN.

C9000 Series

Defaults Enabled

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced

Usage Information The `no default vlan disable` command is not listed in the running-configuration, but when the default VLAN is disabled, `default-vlan disable` is listed in the running-configuration. Use this command in Configuration Terminal Batch mode to disable the default VLAN in a dual-homing setup.

name

Assign a name to the VLAN.

C9000 Series

Syntax `name` *`vlan-name`*

To remove the name from the VLAN, use the `no name` command.

Parameters

vlan-name	Enter up to 32 characters as the name of the VLAN.

Defaults Not configured.

Command Modes INTERFACE VLAN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information To display information about a named VLAN, enter the `show vlan` command with the name parameter or the show interfaces description command.

Related Commands interface vlan — configures a VLAN.

show vlan — displays the current VLAN configurations on the switch.

show config

Display the current configuration of the selected VLAN.

C9000 Series

Syntax `show config`

Command Modes INTERFACE VLAN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(conf-if-vl-100)#show config
!
interface Vlan 100
  no ip address
  no shutdown
Dell(conf-if-vl-100)#
```

show vlan

Display the current VLAN configurations on the switch.

C9000 Series

Syntax `show vlan [brief | id vlan-id | name vlan-name]`

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to display the following information: • VLAN ID • VLAN name (left blank if none is configured) • Spanning Tree Group ID • MAC address aging time • IP address
id *vlan-id*	(OPTIONAL) Enter the keyword `id` and VLAN ID number from 1 to 4094 to display the configuration of the specified VLAN.
name *vlan-name*	(OPTIONAL) Enter the keyword `name` and the name assigned to a VLAN. Only information on the specified VLAN is displayed.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Updated to support OpenFlow.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Augmented to display PVLAN data for the C-Series and S-Series and revised the output to include the Description field to display a user-entered VLAN description.
7.6.1.0	Introduced on the S-Series and revised the output to display Native VLAN.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information The following describes the `show vlan` command shown in the following example.

Column Heading	Description
(Column 1 — no heading)	• asterisk symbol (*) = Default VLAN • G = GVRP VLAN • P = primary VLAN • C = community VLAN • I = isolated VLAN • O = OpenFlow
NUM	Displays existing VLAN IDs.
Status	Displays the word *Inactive* for inactive VLANs and the word *Active* for active VLANs.
Q	• Displays G for GVRP tagged • M for member of a VLAN-Stack VLAN • T for tagged interface • U for untagged interface • x (not capitalized x) for Dot1x untagged • X (capitalized X) for Dot1x tagged • o (not capitalized o) for OpenFlow untagged • O (capitalized O) for OpenFlow tagged • H for VSN tagged • i (not capitalized i) for Internal untagged • I (capitalized I) for Internal tagged • v (not capitalized v) for VLT untagged • V (capitalized V) for VLT tagged
Ports	Displays the type, slot, and port information. • Po = port channel • Te = 10-Gigabit Ethernet • Fo = 40-Gigabit Ethernet

Example

```
Dell#show vlan

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring VLANs, P -
Primary, C - Community, I - Isolated
       O - Openflow
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   o - OpenFlow untagged, O - OpenFlow tagged
   G - GVRP tagged, M - Vlan-stack
   i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT tagged

    NUM    Status    Description                    Q Ports
*   1      Active                                   U Fo 0/0
                                                    U Fo 2/8
    10     Active                                   T Po10(Te 0/140,Te 1/80)
                                                    T Po20(Te 1/81)
    20     Active                                   T Po10(Te 0/140,Te 1/80)
                                                    T Po20(Te 1/81)
    30     Active                                   T Fo 2/0
```

Example (VLAN ID)

```
Dell# show vlan id 20

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring VLANs, P -
Primary, C - Community, I - Isolated
       O - Openflow
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   o - OpenFlow untagged, O - OpenFlow tagged
   G - GVRP tagged, M - Vlan-stack
   i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT tagged

    NUM    Status    Description                    Q Ports
    20     Active                                   T Po10(Te 0/140,Te 1/80)
                                                    T Po20(Te 1/81)
                                                    T Fo 2/0
```

Example (Brief)

```
Dell#show vlan brief
VLAN Name                            STG   MAC Aging IP Address
---- ------------------------------- ----  --------- ------------------
1                                    0     1800      unassigned
10                                   0     1800      unassigned
20                                   0     1800      2.3.3.3/24
30                                   0     1800      2.1.1.1/24
```

Example (Name)

```
Dellconf)#interface vlan 20
Dell(conf-if-vl-20)#name test
Dell(conf-if-vl-20)#do show vlan name test

Codes: * - Default VLAN, G - GVRP VLANs, R - Remote Port Mirroring VLANs, P -
Primary, C - Community, I - Isolated
       O - Openflow
Q: U - Untagged, T - Tagged
   x - Dot1x untagged, X - Dot1x tagged
   o - OpenFlow untagged, O - OpenFlow tagged
   G - GVRP tagged, M - Vlan-stack
   i - Internal untagged, I - Internal tagged, v - VLT untagged, V - VLT tagged

    NUM    Status    Description                    Q Ports
    20     Active                                   T Po10(Te 0/140,Te 1/80)
                                                    T Po20(Te 1/81)
                                                    T Fo 2/0
```

Related Commands

interface vlan — configures a VLAN.

tagged

Add a Layer 2 interface to a VLAN as a tagged interface.

C9000 Series

Syntax

`tagged` *`interface`*

To remove a tagged interface from a VLAN, use the `no tagged` *`interface`* command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults

All interfaces in Layer 2 mode are untagged.

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

When you use the `no tagged` command, the interface is automatically placed in the Default VLAN as an untagged interface unless the interface is a member of another VLAN. If the interface belongs to several VLANs, remove it from all VLANs to change it to an untagged interface.

Tagged interfaces can belong to multiple VLANs, while untagged interfaces can only belong to one VLAN at a time.

Related Commands

interface vlan — configures a VLAN.

untagged — specifies which interfaces in a VLAN are untagged.

track ip

Track the Layer 3 operational state of a Layer 3 VLAN, using a subset of the VLAN member interfaces.

C9000 Series

Syntax

`track ip` *`interface`*

To remove the tracking feature from the VLAN, use the `no track ip` *`interface`* command.

Parameters

interface — Enter the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

Not configured.

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

When this command is configured, the VLAN is operationally UP if any of the interfaces specified in the `track ip` command are operationally UP, and the VLAN is operationally DOWN if none of the tracking interfaces are operationally UP.

If the `track ip` command is not configured, the VLAN's Layer 3 operational state depends on all the members of the VLAN.

The Layer 2 state of the VLAN, and hence the Layer 2 traffic, is not affected by the `track ip` command configuration.

Related Commands

interface vlan — configures a VLAN.

tagged — specifies which interfaces in a VLAN are tagged.

untagged

Add a Layer 2 interface to a VLAN as an untagged interface.

C9000 Series

Syntax

`untagged` *`interface`*

To remove an untagged interface from a VLAN, use the `no untagged` *`interface`* command.

Parameters

interface

Enter the following keywords and slot/port or number information:

- For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255;

the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults All interfaces in Layer 2 mode are untagged.

Command Modes INTERFACE VLAN

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information Untagged interfaces can only belong to one VLAN.

In the Default VLAN, you cannot use the `no untagged interface` command. To remove an untagged interface from all VLANs, including the Default VLAN, enter INTERFACE mode and use the `no switchport` command.

Related Commands

- interface vlan — configures a VLAN.
- tagged — specifies which interfaces in a VLAN are tagged.

Far-End Failure Detection (FEFD)

The Dell Networking operating software supports far-end failure detection (FEFD) on the Ethernet interfaces.

The FEFD feature detects and reports far-end link failures.

- FEFD is not supported on the Management interface.
- During an RPM failover, FEFD is operationally disabled for approximately 8 to 10 seconds.
- By default, FEFD is disabled.

debug fefd

Enable debugging of FEFD.

C9000 Series

Syntax

`debug fefd {events | packets} [interface]`

To disable debugging of FEFD, use the `no debug fefd {events | packets} [interface]` command.

Parameters

events	Enter the keyword `events` to enable debugging of FEFD state changes.
packets	Enter the keyword `packets` to enable debugging of FEFD to view information on packets sent and received.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Related Commands

- fefd — enables far-end failure detection on an interface.
- fefd reset — enables FEFD globally on the system.

fefd

Enable Far-End Failure Detection on an interface, set the FEFD interval, or select the FEFD mode.

C9000 Series

Syntax

```
fefd {disable|interval|mode {aggressive|normal}
```

Parameters

disable	Enter the keyword **disable** to disable FEFD for the specified interface.
interval	Enter the keyword **interval**, followed by a value to specify the FEFD interval in seconds. Range is from 3 to 300. Default is 15.
mode	Enter the keyword **mode** followed by the mode type to specify the FEFD mode. • **normal**: Change the link state to "unknown" when a far-end failure is detected by the software on that interface. When the interface is placed in an "unknown" state, the software brings down the line protocol. • **aggressive**: Change the link state to "error-disabled" when a far-end failure is detected by the software on that interface. When an interface is placed in an "error-disabled" state, you must enter the `fefd reset` command to reset the interface state. Range is normal or aggressive. Default is normal.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Usage Information

When you enter `no fefd` for an interface and `fefd-global`, FEFD is enabled on the interface because the `no fefd` command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the `fefd reset` command.

Related Commands

- fefd disable — disables far-end failure detection on an interface.
- fefd reset — enables FEFD globally on the system.
- fefd mode — changes FEFD mode on an interface.

fefd disable

Disable FEFD on an interface only. This command overrides the `fefd reset` command for the interface.

C9000 Series

Syntax

`fefd disable`

To re-enable FEFD on an interface, use the `no fefd disable` command.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information

When you enter `no fefd` for an interface and fefd-global, FEFD is enabled on the interface because the `no fefd` command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the `fefd reset` command.

Related Commands

- fefd reset — enables FEFD globally on the system.
- fefd mode — changes FEFD mode on an interface.

fefd interval

Set an interval between control packets.

C9000 Series

Syntax

`fefd interval` *`seconds`*

To return to the default value, use the `no fefd interval` command.

Parameters

seconds	Enter a number as the time between FEFD control packets. The range is from 3 to 255 seconds. The default is **15 seconds**.

Defaults **15 seconds**

Command Modes INTERFACE

Command History The following is the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related Commands

- fefd — enables far-end failure detection.

fefd mode

Change the FEFD mode on an interface.

C9000 Series

Syntax `fefd mode {normal | aggressive}]`

To return the FEFD mode to the default of normal, use the `no fefd mode` command.

Parameters

normal	(OPTIONAL) Enter the keyword `normal` to change the link state to "unknown" when a far-end failure the software detects on that interface. When the interface is placed in "unknown" state, the software brings down the line protocol.
aggressive	(OPTIONAL) Enter the keyword `aggressive` to change the link state to "error-disabled" when a far-end failure the software detects on that interface. When an interface is placed in "error-disabled" state, enter the `fefd reset` command to reset the interface state.

Defaults normal

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related Commands

- fefd — enables far-end failure detection.

fefd reset

Reset all interfaces or a single interface that was in "error-disabled" mode.

C9000 Series

Syntax `fefd reset [interface]`

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults Not configured.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Related Commands

- fefd — enables far-end failure detection.

fefd-global interval

Configure an interval between FEFD control packets.

C9000 Series

Syntax

`fefd-global interval seconds`

To return to the default value, use the `no fefd-global interval` command.

Parameters

seconds	Enter a number as the time between FEFD control packets. The range is from 3 to 300 seconds. The default is **15 seconds**.

Defaults

15 seconds

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related Commands

- fefd — enables far-end failure detection.
- fefd-global — enables FEFD globally on the system.

fefd-global

Enable FEFD globally on the system.

C9000 Series

Syntax

`fefd-global [interval seconds][mode {normal | aggressive}]`

To disable FEFD globally, use the `no fefd-global [mode {normal | aggressive}]` command.

Parameters

interval *seconds*	Enter the keyword `interval` followed by the number of seconds to wait between FEFD control packets. Range is from 3 to 300 seconds. Default is 15 seconds.

	normal	(OPTIONAL) Enter the keywords `mode normal` to change the link state to "unknown" when a far-end failure the software detects on that interface. When the interface is placed in "unknown" state, the software brings down the line protocol. The default is **Normal mode**.
	aggressive	(OPTIONAL) Enter the keywords `mode aggressive` to change the link state to "error-disabled" when a far-end failure the software detects on that interface. When an interface is placed in "error-disabled" state, t enter the `fefd reset` command to reset the interface state.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Usage Information If you enter only the `fefd-global` syntax, the mode is normal and the default interval is 15 seconds.

If you disable FEFD globally (`no fefd-global`), the system does not remove the FEFD interface configuration.

Related Commands

- fefd — enables far-end failure detection.
- fefd-global interval — configures an interval between FEFD control packets.
- show fefd — shows the FEFD command output.

show fefd

View FEFD status globally or on a specific interface.

C9000 Series

Syntax `show fefd [interface]`

Parameters

interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.

Usage Information

The following describes the `show fefd` command shown in the following example.

Field	Description
Interface	Displays the interfaces type and number.
Mode	Displays the mode (aggressive or normal) or NA if the interface contains `fefd reset` in its configuration.
Interval	Displays the interval between FEFD packets.
State	Displays the state of the interface and can be one of the following: • bi-directional (interface is up, connected and hearing neighbor's echoes). • err-disabled (only found when FEFD mode is aggressive and when the interface has not hearing its neighbor's echoes for three times the message interval. To reset an interface in this state, use the `fefd reset` command.) • unknown (only found when FEFD mode is normal. • locally disabled (interface contains the `fefd reset` command in its configuration). • Admin Shutdown (interface is disabled with the `shutdown` command).

Example

```
Dell#sh fefd
FEFD is globally 'ON', interval is 10 seconds, mode is 'Aggressive'.

INTERFACE MODE       INTERVAL   STATE
                     (second)
Te 1/0   Aggressive  10         Admin Shutdown
Te 1/1   Aggressive  10         Admin Shutdown
Te 1/2   Aggressive  10         Admin Shutdown
Te 1/3   Aggressive  10         Admin Shutdown
Te 1/4   Aggressive  10         Admin Shutdown
Te 1/5   Aggressive  10         Admin Shutdown
Te 1/6   Aggressive  10         Admin Shutdown
Te 1/7   Aggressive  10         Admin Shutdown
Te 1/8   Aggressive  10         Admin Shutdown
Te 1/9   Aggressive  10         Admin Shutdown
Te 1/10  NA          NA         Locally disabled
```

```
Te 1/11  Aggressive  10         Err-disabled
Dell#
```

Related Commands

- fefd — enables far-end failure detection.
- fefd disable — disables FEFD on an interface only.
- fefd-global — enables FEFD globally on the system.
- fefd reset — resets all interfaces or a single interface that was in “error-disabled” mode.

31

Link Aggregation Control Protocol (LACP)

This chapter contains commands for Dell Networks's implementation of the link aggregation control protocol (LACP) for creating dynamic link aggregation groups (LAGs) — known as "port-channels" in the Dell Networking operating software.

NOTE: For static LAG commands, refer to Port Channel Commands in the Interfaces chapter), based on the standards specified in the IEEE 802.3 Carrier sense multiple access with collision detection (CSMA/CD) access method and physical layer specifications.

Topics:

- clear lacp counters
- debug lacp
- lacp long-timeout
- lacp port-priority
- lacp system-priority
- port-channel mode
- port-channel-protocol lacp
- show lacp

clear lacp counters

Clear port channel counters.

C9000 Series

Syntax

```
clear lacp port-channel-number counters
```

Parameters

port-channel-number	Enter a port-channel number. The range is from 1 to 128.

Defaults

Without a Port Channel specified, the command clears all Port Channel counters.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands show lacp — displays the LACP configuration.

debug lacp

Debug LACP (configuration, events, and so on).

C9000 Series

Syntax `debug lacp {config | events | pdu [interface-type [in | out]]}`

To disable LACP debugging, use the `no debug {config | events | pdu [interface-type [in | out]]}` command.

Parameters

config	(OPTIONAL) Enter the keyword `config` to debug the LACP configuration.
events	(OPTIONAL) Enter the keyword `events` to debug the LACP event information.
pdu	(OPTIONAL) Enter the keyword `pdu` to debug the LACP Protocol Data Unit information.
***interface-type* in | out**	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information. • For a Ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE. Optionally, enter an `in` or `out` parameter: • Receive enter `in` • Transmit enter `out`

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

lacp long-timeout

Configure a long timeout period (30 seconds) for an LACP session.

C9000 Series

Syntax

`lacp long-timeout`

To reset the timeout period to a short timeout (1 second), use the `no lacp long-timeout` command.

Defaults

1 second

Command Modes

INTERFACE (conf-if-po-number)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information This command applies to dynamic port-channel interfaces only. When applied on a static port-channel, this command has no effect.

Related Commands show lacp — displays the LACP configuration.

lacp port-priority

To influence which ports will be put in Standby mode when there is a hardware limitation that prevents all compatible ports from aggregating, configure the port priority.

C9000 Series

Syntax `lacp port-priority` *`priority-value`*

To return to the default setting, use the `no lacp port-priority` *`priority-value`* command.

Parameters

priority-value	Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is **32768**.

Defaults **32768**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

lacp system-priority

Configure the LACP system priority.

C9000 Series

Syntax `lacp system-priority priority-value`

Parameters

priority-value	Enter the port-priority value. The higher the value number, the lower the priority. The range is from 1 to 65535. The default is **32768**.

Defaults **32768**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

port-channel mode

Configure the LACP port channel mode.

C9000 Series

Syntax `port-channel number mode [active] [passive] [off]`

Parameters

number	Enter the keywords `number` then a number.
active	Enter the keyword `active` to set the mode to the active state.

NOTE: LACP modes are defined in *Usage Information*.

passive	Enter the keyword `passive` to set the mode to the passive state. **NOTE: LACP modes are defined in *Usage Information*.**
off	Enter the keyword `off` to set the mode to the off state. **NOTE: LACP modes are defined in *Usage Information*.**

Defaults **off**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information LACP Modes

Mode	Function
active	An interface is in an active negotiating state in this mode. LACP runs on any link configured in the active state and also automatically initiates negotiation with other ports by initiating LACP packets.
passive	An interface is not in an active negotiating state in this mode. LACP runs on any link configured in the passive state. Ports in a passive state respond to negotiation requests from other ports that are in active states. Ports in a passive state respond to LACP packets
off	An interface cannot be part of a dynamic port channel in off mode. LACP does not run on a port configured in off mode.

port-channel-protocol lacp

Enable LACP on any LAN port.

C9000 Series

Syntax `port-channel-protocol lacp`

To disable LACP on a LAN port, use the `no port-channel-protocol lacp` command.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced on the E-Series.

Related Commands

- show lacp — displays the LACP information.
- show interfaces port-channel — displays information on configured Port Channel groups.

show lacp

Display the LACP matrix.

C9000 Series

Syntax `show lacp port-channel-number [sys-id | counters]`

Parameters

port-channel-number	Enter a port-channel number. The range is from 1 to 128.
sys-id	(OPTIONAL) Enter the keywords `sys-id` and the value that identifies a system.
counters	(OPTIONAL) Enter the keyword `counters` to display the LACP counters.

Defaults Without a Port Channel specified, the command clears all Port Channel counters.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example (Port-Channel-Number)

```
Dell#show lacp 1
Port-channel 1 admin up, oper up, mode lacp
Actor   System ID:Priority 32768, Address 0001.e800.a12b
Partner System ID:Priority 32768, Address 0001.e801.45a5
                  Actor Admin Key 1, Oper Key 1, Partner Oper Key 1
                  LACP LAG 1 is an aggregatable link

A-Active LACP, B-Passive LACP, C-Short Timeout, D-Long Timeout
E-Aggregatable Link, F-Individual Link, G-IN_SYNC, H-OUT_OF_SYNC
I-Collection enabled, J-Collection disabled, K-Distribution enabled L-
Distribution disabled,
M-Partner Defaulted, N-Partner Non-defaulted, O-Receiver is in expired state,
P-Receiver is not in expired state

Port Te 1/6 is enabled, LACP is enabled and mode is lacp
  Actor   Admin: State ACEHJLMP Key 1    Priority 128
           Oper: State ACEGIKNP Key 1    Priority 128
  Partner Admin: State BDFHJLMP Key 0    Priority 0
           Oper: State BCEGIKNP Key 1    Priority 128
Dell#
```

Example (Sys-id)

```
Dell#show lacp 1 sys-id
Actor    System ID: Priority 32768, Address 0001.e800.a12b
Partner  System ID: Priority 32768, Address 0001.e801.45a5

Dell#
```

Example (Counter)

```
Dell#show lacp 1 counters
---------------------------------------------------
           LACP PDU    Marker PDU   Unknown   Illegal
Port     Xmit Recv   Xmit Recv      Pkts Rx   Pkts Rx
---------------------------------------------------
Te 1/6   200  200     0    0        0          0
Dell#
```

Related Commands

- clear lacp counters — clears the LACP counters.
- show interfaces port-channel — displays information on configured Port Channel groups.

32

Link Layer Discovery Protocol (LLDP)

Link layer discovery protocol (LLDP) advertises connectivity and management from the local station to the adjacent stations on an IEEE 802 LAN.

This chapter contains the following sections:

- LLPD Commands
- LLDP-MED Commands

LLDP facilitates multi-vendor interoperability by using standard management tools to discover and make available a physical topology for network management. The Dell Networking operating system implementation of LLDP is based on IEEE standard 801.1ab.

The starting point for using LLDP is invoking LLDP with the `protocol lldp` command in either CONFIGURATION or INTERFACE mode.

The information LLDP distributes is stored by its recipients in a standard management information base (MIB). You can access the information by a network management system through a management protocol such as simple network management protocol (SNMP).

Topics:

- LLPD Commands
- snmp-notification-interval
- LLDP-MED Commands

LLPD Commands

The following are LLDP commands.

advertise dot1-tlv

Advertise dot1 TLVs (Type, Length, Value).

C9000 Series

Syntax

`advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name}`

To remove advertised dot1-tlv, use the `no advertise dot1-tlv {port-protocol-vlan-id | port-vlan-id | vlan-name}` command.

Parameters

port-protocol-vlan-id	Enter the keywords `port-protocol-vlan-id` to advertise the port protocol VLAN identification TLV.
port-vlan-id	Enter the keywords `port-vlan-id` to advertise the port VLAN identification TLV.
vlan-name	Enter the keywords `vlan-name` to advertise the vlan-name TLV. This keyword is only supported on the C-Series and S-Series.

Defaults Disabled.

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series. Added the `vlan-name` option.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands protocol lldp (Configuration) — enables LLDP globally.

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise dot3-tlv

Advertise dot3 TLVs (Type, Length, Value).

C9000 Series

Syntax `advertise dot3-tlv {max-frame-size}`

To remove advertised dot3-tlv, use the `no advertise dot3-tlv {max-frame-size}` command.

Parameters

max-frame-size Enter the keywords `max-frame-size` to advertise the dot3 maximum frame size.

Defaults none

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

advertise interface-port-desc

Advertise port descriptor.

Syntax

```
advertise interface-port-desc {description | port-id}
```

To remove the advertised port descriptor, use the `no advertise interface—port—desc {description | port-id}` command.

Parameters

description	Enter the keyword `description` then the interface description.
port-id	Enter the keyword `port-id` then the port-id. The range is from 0 to 7.

Defaults

None

Command Modes

CONFIGURATION (conf-lldp)

INTERFACE (conf-if-*interface*-lldp)

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(2.0P2)	Introduced the `description` and `port-id` options.

Usage Information

If you do not specify the option, by default the port-id takes higher precedence and sends the port-id in the LLDP packets.

advertise dot3-tlv

Configure the system or an interface to advertise IEEE 802.3at extended power-via-mdi.

C9000 Series

Syntax

```
advertise dot3-tlv power-via-mdi
```

To remove the advertised dot3–tlv, use the `no advertise dot3-tlv power-via-mdi` command

Parameters

power-via-mdi	Enter the keyword `power–via-mdi` to advertise IEEE 802.3at power-via-mdi TLV.

Defaults

Disabled

Command Modes

- LLDP CONFIGURATION (conf-lldp)
- INTERFACE LLDP CONFIGURATION (conf-if-*interface*-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

The `advertise dot3-tlv power–via–mdi` command enables the system to advertise IEEE 802.3at power-via-mdi TLV to advertise its power negotiation capabilities with the powered devices via Link Layer Discovery Protocol (LLDP). You can configure this command either on a specific interface or globally.

Example

```
Dell(conf)#interface peGigE 0/0/0
Dell(conf-if-pegi-0/0/0)#protocol lldp
Dell(conf-if-pegi-0/0/0-lldp)#advertise dot3-tlv power-via-mdi
Dell(conf-if-pegi-0/0/0-lldp)#
```

advertise management-tlv

Advertise management TLVs (Type, Length, Value).

C9000 Series

Syntax

```
advertise management-tlv {management-address | system-capabilities | system-description | system-name}
```

To remove advertised management TLVs, use the `no advertise management-tlv {management-address | system-capabilities | system-description | system-name}` command.

Parameters

management-address	Enter the keyword management-address to advertise the management IP address TLVs to the LLDP peer.
system-capabilities	Enter the keywords `system-capabilities` to advertise the system capabilities TLVs to the LLDP peer.
system-description	Enter the keywords `system-description` to advertise the system description TLVs to the LLDP peer.
system-name	Enter the keywords `system-name` to advertise the system name TLVs to the LLDP peer.

Defaults none

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Modified to support management-address parameter.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information The command options `management-address`,`system-capabilities`, `system-description`, and `system-name` can be invoked individually or together, in any sequence.

advertise management-tlv (Interface)

Advertise management type, length, values (TLVs) to the specified interface.

C9000 Series

Syntax

```
advertise management-tlv {management-address | system-capabilities | system-description | system-name}
```

To remove advertised management TLVs, use the `no advertise management-tlv {management-address | system-capabilities | system-description | system-name}` command.

Parameters

management-address	Enter the keywords `management-address` to advertise the management IP address TLVs to the specified interface.
system-capabilities	Enter the keywords `system-capabilities` to advertise the system capabilities TLVs to the specified interface.
system-description	Enter the keywords `system-description` to advertise the system description TLVs to the specified interface.
system-name	Enter the keywords `system-name` to advertise the system name TLVs to the specified interface.

Defaults none

Command Modes INTERFACE (conf-*interface*-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the Z9000 and S4810.
8.3.19.0	Introduced on the S4820T.

clear lldp counters

Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

C9000 Series

Syntax `clear lldp counters` *interface*

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the *slot/port* information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Management Ethernet interface, enter the keyword `managementethernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information. • For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255;

the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

clear lldp neighbors

Clear LLDP neighbor information for all interfaces or a specific interface.

C9000 Series

Syntax `clear lldp neighbors {`*`interface`*`}`

Parameters

interface Enter the following keywords and slot/port or number information:

- For a 1–Gigabit Ethernet interface, enter the keyword `gigabitethernet` then the slot/ port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/ port information.
- For a Management Ethernet interface, enter the keyword `managementethernet` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255;

the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

debug lldp interface

To display timer events, neighbor additions or deletions, and other information about incoming and outgoing packets, enable LLDP debugging.

Syntax `debug lldp interface {`*`interface`* `| all}{events | packet {brief | detail} {tx | rx | both}}`

To disable debugging, use the `no debug lldp [interface {`*`interface`* `| all}{events} {packet {brief | detail} {tx | rx | both}}]` command.

Parameters

interface *interface* Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

all Enter the keyword `all` to display information on all interfaces.

events	Enter the keyword `events` to display major events such as timer events.
packet	Enter the keyword `packet` to display information regarding packets coming in or going out.
brief	Enter the keyword `brief` to display brief packet information.
detail	Enter the keyword `detail` to display detailed packet information.
tx	Enter the keyword `tx` to display transmit-only packet information.
rx	Enter the keyword `rx` to display receive-only packet information.
both	Enter the keyword `both` to display both receive and transmit packet information.

Defaults None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13.0.0	Enhanced to display organizational specific unrecognized LLDP TLVs.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on the E-Series.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
DellEMC#Dec  4 22:38:27 : Received LLDP pkt on TenGigabitEthernet 1/1 of
length 204 :
Dec  4 22:38:27 : Packet dump:
Dec  4 22:38:27 :  01 80 c2 00 00 0e 00 a0 c9 00 00 03 81 00 00 00
Dec  4 22:38:27 :  88 cc 02 07 04 00 a0 c9 00 00 01 04 02 05 54 06
Dec  4 22:38:27 :  02 01 2c fe 05 aa bb cc 04 61 fa 01 40 00 00 00
Dec  4 22:38:28 :  00 00 00 00 00 00 00 00 c6 0f ba 27
Dec  4 22:38:28 : TLV: Chassis ID, Len: 7, Subtype: Mac address (4) Value:
```

```
00:a0:c9:00:00:01
Dec  4 22:38:29 : TLV: Port ID, Len: 2, Subtype: Interface name (5) Value: T
Dec  4 22:38:29 : TLV: TTL, Len: 2, Value: 300
Dec  4 22:38:29 : TLV: UNKNOWN TLV, ORG_SPEC[aa-bb-cc, 4], Len: 1, Value:a
Dec  4 22:38:29 :  aa bb cc 04 61
Dec  4 22:38:29 :  40
Dec  4 22:38:29 : TLV: UNKNOWN TLV, Type: 125 Len: 1, Value: @
Dec  4 22:38:29 : TLV: ENDOFPDU, Len: 0
```

disable

Enable or disable LLDP.

C9000 Series

Syntax

`disable`

To enable LLDP, use the `no disable` command.

Defaults

Enabled, that is no disable.

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands

protocol lldp (Configuration) — enables LLDP globally.

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

hello

Configure the rate at which the LLDP control packets are sent to its peer.

C9000 Series

Syntax

`hello seconds`

To revert to the default, use the `no hello seconds` command.

Parameters

seconds	Enter the rate, in seconds, at which the control packets are sent to its peer. The rate is from 5 to 180 seconds. The default is **30 seconds**.

Defaults

30 seconds

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

management-interface

Enable and configure LLDP protocol parameters on the management interface.

C9000 Series

Syntax

`management-interface`

To remove LLDP configuration on a management interface, use the `no management-interface` command.

Command Modes

LLDP (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Introduced on the Z9000 and S4810.

Usage Information

To enable LLDP on the management interface, use the `no disable` command in LLDP-MANAGEMENT-INTERFACE mode (conf-lldp-mgmtIf).

mode

To receive or transmit, set LLDP.

C9000 Series

Syntax

`mode {tx | rx}`

To return to the default, use the `no mode {tx | rx}` command.

Parameters

tx	Enter the keyword `tx` to set the mode to transmit.
rx	Enter the keyword `rx` to set the mode to receive.

Defaults

Both **transmit** and **receive**.

Command Modes

CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands protocol lldp (Configuration) — enables LLDP globally.

show lldp neighbors — displays the LLDP neighbors.

multiplier

Set the number of consecutive misses before LLDP declares the interface dead.

C9000 Series

Syntax `multiplier integer`

To return to the default, use the `no multiplier integer` command.

Parameters

integer	Enter the number of consecutive misses before the LLDP declares the interface dead. The range is from 2 to 10.

Defaults **4 x hello**

Command Modes CONFIGURATION (conf-lldp) and INTERFACE (conf-if-*interface*-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

protocol lldp (Configuration)

Enable the LLDP globally on the switch.

C9000 Series

Syntax `protocol lldp`

To disable LLDP globally on the chassis, use the `no protocol lldp` command.

Defaults Enabled.

Command Modes CONFIGURATION(conf-lldp)

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

protocol lldp (Interface)

Enter the LLDP protocol in INTERFACE mode.

C9000 Series

Syntax `[no] protocol lldp`

To return to the global LLDP configuration mode, use the `no protocol lldp` command from Interface mode.

Defaults LLDP is not enabled on the interface.

Command Modes INTERFACE (conf-if-*interface*-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

Before LLDP can be configured on an interface, it must be enabled globally from CONFIGURATION mode. This command places you in LLDP mode on the interface; it does not enable the protocol.

When you enter the `LLDP` protocol in the Interface context, it overrides global configurations. When you execute the `no protocol lldp` from INTERFACE mode, interfaces begin to inherit the configuration from global LLDP CONFIGURATION mode.

show lldp neighbors

Display LLDP neighbor information for all interfaces or a specified interface.

Syntax

```
show lldp neighbors [interface interface] [detail]
```

Parameters

interface *interface*

(OPTIONAL) Enter the following keywords and the interface information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

detail

(OPTIONAL) Enter the keyword `detail` to display all the TLV information, remote management IP addresses, timers, and LLDP tx and rx counters.

Defaults

None

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.13.0.0	Enhanced to display organizational specific unrecognized LLDP TLVs.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.1.(0.0)	Modified output of detail parameter to display remote management IP addresses.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on the E-Series.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information Omitting the keyword `detail` displays only the remote chassis ID, Port ID, and Dead Interval.

Example

```
DellEMC(conf-if-te-1/31)# do show lldp neighbors
Loc PortID Rem  Host Name       Rem     Port Id Rem Chassis Id
-----------------------------------------------------------------
Te   1/21    R2  TenGigabitEthernet  2/11   00:01:e8:06:95:3e
Te   1/31    R3  TenGigabitEthernet  3/11   00:01:e8:09:c2:4a
```

Example (Detail)

```
DellEMC(conf)#do show lldp neighbors detail
================================================================================
Local Interface TenGigabitEthernet 1/1 has 2 neighbors
  Total Frames Out: 3
  Total Frames In: 8
  Total Neighbor information Age outs: 0
  Total Multiple Neighbors Detected: 0
  Total Frames Discarded: 0
  Total In Error Frames: 0
  Total Unrecognized TLVs: 960
  Total TLVs Discarded: 16
  Next packet will be sent after 9 seconds
  The neighbors are given below:
  ------------------------------------------------------------------------------

    Remote Chassis ID Subtype: Mac address (4)
    Remote Chassis ID:  00:00:00:00:00:01
    Remote Port Subtype:  Interface name (5)
    Remote Port ID:  TenGigabitEthernEt 1/40
    Local Port ID: TenGigabitEthernet 1/1
    Locally assigned remote Neighbor Index: 1
    Remote TTL:  120
    Information valid for next 44 seconds
    Time since last information change of this neighbor:  00:01:16
    UnknownTLVList:
          (  9,  4) ( 10,  4) ( 11,  4) ( 12,  4) ( 13,  4) ( 14,  4) ( 15,  4) ( 16,  4) ( 17,  4) ( 18,  4)
          ( 19,  4) ( 20,  4) ( 21,  4) ( 22,  4) ( 23,  4) ( 24,  4) ( 25,  4) ( 26,  4) ( 27,  4) ( 28,  4)
          ( 29,  4) ( 30,  4) ( 31,  4) ( 32,  4) ( 33,  4) ( 34,  4) ( 35,  4) ( 36,  4) ( 37,  4) ( 38,  4)
```

```
        ( 39,  4) ( 40,  4) ( 41,  4) ( 42,  4) ( 43,  4) ( 44,  4) ( 45,  4) ( 46,  4) ( 47,  4) ( 48,  4)
        ( 49,  4) ( 50,  4) ( 51,  4) ( 52,  4) ( 53,  4) ( 54,  4) ( 55,  4) ( 56,  4) ( 57,  4) ( 58,  4)
        ( 59,  4) ( 60,  4) ( 61,  4) ( 62,  4) ( 63,  4) ( 64,  4) ( 65,  4) ( 66,  4) ( 67,  4) ( 68,  4)
        ( 69,  4) ( 70,  4) ( 71,  4) ( 72,  4) ( 73,  4) ( 74,  4) ( 75,  4) ( 76,  4) ( 77,  4) ( 78,  4)
        ( 79,  4) ( 80,  4) ( 81,  4) ( 82,  4) ( 83,  4) ( 84,  4) ( 85,  4) ( 86,  4) ( 87,  4) ( 88,  4)
        ( 89,  4) ( 90,  4) ( 91,  4) ( 92,  4) ( 93,  4) ( 94,  4) ( 95,  4) ( 96,  4) ( 97,  4) ( 98,  4)
        ( 99,  4) (100,  4) (101,  4) (102,  4) (103,  4) (104,  4) (105,  4) (106,  4) (107,  4) (108,  4)
        (109,  4) (110,  4) (111,  4) (112,  4) (113,  4) (114,  4) (115,  4) (116,  4) (117,  4) (118,  4)
        (119,  4) (120,  4) (121,  4) (122,  4) (123,  4) (124,  4) (125,  4) (126,  4)
  OrgUnknownTLVList:
 ------------------------------------------------------------------------------

  Remote Chassis ID Subtype: Mac address (4)
  Remote Chassis ID:  00:00:00:00:00:02
  Remote Port Subtype:  Interface name (5)
  Remote Port ID:  TenGigabitEthernEt 1/40
  Local Port ID: TenGigabitEthernet 1/1
  Locally assigned remote Neighbor Index: 2
  Remote TTL:  120
  Information valid for next 43 seconds
  Time since last information change of this neighbor:  00:01:17
  UnknownTLVList:
        (  9,  4) ( 10,  4) ( 11,  4) ( 12,  4) ( 13,  4) ( 14,  4) ( 15,  4) ( 16,  4) ( 17,  4) ( 18,  4)
        ( 19,  4) ( 20,  4) ( 21,  4) ( 22,  4) ( 23,  4) ( 24,  4) ( 25,  4) ( 26,  4) ( 27,  4) ( 28,  4)
        ( 29,  4) ( 30,  4) ( 31,  4) ( 32,  4) ( 33,  4) ( 34,  4) ( 35,  4) ( 36,  4) ( 37,  4) ( 38,  4)
        ( 39,  4) ( 40,  4) ( 41,  4) ( 42,  4) ( 43,  4) ( 44,  4) ( 45,  4) ( 46,  4) ( 47,  4) ( 48,  4)
        ( 49,  4) ( 50,  4) ( 51,  4) ( 52,  4) ( 53,  4) ( 54,  4) ( 55,  4) ( 56,  4) ( 57,  4) ( 58,  4)
        ( 59,  4) ( 60,  4) ( 61,  4) ( 62,  4) ( 63,  4) ( 64,  4) ( 65,  4) ( 66,  4) ( 67,  4) ( 68,  4)
        ( 69,  4) ( 70,  4) ( 71,  4) ( 72,  4) ( 73,  4) ( 74,  4) ( 75,  4) ( 76,  4) ( 77,  4) ( 78,  4)
        ( 79,  4) ( 80,  4) ( 81,  4) ( 82,  4) ( 83,  4) ( 84,  4) ( 85,  4) ( 86,  4) ( 87,  4) ( 88,  4)
        ( 89,  4) ( 90,  4) ( 91,  4) ( 92,  4) ( 93,  4) ( 94,  4) ( 95,  4) ( 96,  4) ( 97,  4) ( 98,  4)
        ( 99,  4) (100,  4) (101,  4) (102,  4) (103,  4) (104,  4) (105,  4) (106,  4) (107,  4) (108,  4)
        (109,  4) (110,  4) (111,  4) (112,  4) (113,  4) (114,  4) (115,  4) (116,  4) (117,  4) (118,  4)
        (119,  4) (120,  4) (121,  4) (122,  4) (123,  4) (124,  4) (125,  4) (126,  4)
  OrgUnknownTLVList:
 ------------------------------------------------------------------------------

==============================================================================
Local Interface TenGigabitEthernet 1/2 has 3 neighbors
  Total Frames Out: 4
  Total Frames In: 8
  Total Neighbor information Age outs: 0
  Total Multiple Neighbors Detected: 0
  Total Frames Discarded: 0
  Total In Error Frames: 0
  Total Unrecognized TLVs: 1056
  Total TLVs Discarded: 0
  Next packet will be sent after 16 seconds
  The neighbors are given below:
 ------------------------------------------------------------------------------

   Remote Chassis ID Subtype: Mac address (4)
   Remote Chassis ID:  4c:76:25:f4:ab:01
   Remote Port Subtype:  Interface name (5)
   Remote Port ID:  fortyGigE 1/2/8/1
   Local Port ID: TenGigabitEthernet 1/2
   Locally assigned remote Neighbor Index: 1
   Remote TTL:  300
   Information valid for next 201 seconds
   Time since last information change of this neighbor:  00:01:39
   UnknownTLVList:
   OrgUnknownTLVList:
        ((00-01-66),127,  4) ((00-01-66),126,  4) ((00-01-66),125,  4) ((00-01-66),124,  4) ((00-01-66),123,  4)
        ((00-01-66),122,  4) ((00-01-66),121,  4) ((00-01-66),120,  4) ((00-01-66),119,  4) ((00-01-66),118,  4)
  ------------------------------------------------------------------------------

   Remote Chassis ID Subtype: Mac address (4)
   Remote Chassis ID:  4c:76:25:f4:ab:02
   Remote Port Subtype:  Interface name (5)
   Remote Port ID:  fortyGigE 1/2/8/1
   Local Port ID: TenGigabitEthernet 1/2
   Locally assigned remote Neighbor Index: 2
   Remote TTL:  300
   Information valid for next 201 seconds
   Time since last information change of this neighbor:  00:01:39
   UnknownTLVList:
   OrgUnknownTLVList:
        ((00-01-66),127,  4) ((00-01-66),126,  4) ((00-01-66),125,  4) ((00-01-66),124,  4) ((00-01-66),123,  4)
        ((00-01-66),122,  4) ((00-01-66),121,  4) ((00-01-66),120,  4) ((00-01-66),119,  4) ((00-01-66),118,  4)
  ------------------------------------------------------------------------------

   Remote Chassis ID Subtype: Mac address (4)
   Remote Chassis ID:  4c:76:25:f4:ab:03
   Remote Port Subtype:  Interface name (5)
   Remote Port ID:  fortyGigE 1/2/8/1
   Local Port ID: TenGigabitEthernet 1/2
   Locally assigned remote Neighbor Index: 3
   Remote TTL:  300
   Information valid for next 199 seconds
   Time since last information change of this neighbor:  00:01:41
   UnknownTLVList:
   OrgUnknownTLVList:
        ((00-01-66),127,  4) ((00-01-66),126,  4) ((00-01-66),125,  4) ((00-01-66),124,  4) ((00-01-66),123,  4)
        ((00-01-66),122,  4) ((00-01-66),121,  4) ((00-01-66),120,  4) ((00-01-66),119,  4) ((00-01-66),118,  4)
  ------------------------------------------------------------------------------
```

Example (Detail) for a single interface

```
DellEMC(conf)#do show lldp neighbors interface TenGigabitEthernet 1/1 detail
================================================================================
Local Interface TenGigabitEthernet 1/1 has 3 neighbors
  Total Frames Out: 4
  Total Frames In: 8
  Total Neighbor information Age outs: 0
  Total Multiple Neighbors Detected: 0
  Total Frames Discarded: 0
  Total In Error Frames: 0
  Total Unrecognized TLVs: 1056
  Total TLVs Discarded: 0
  Next packet will be sent after 16 seconds
  The neighbors are given below:
  ------------------------------------------------------------------------------

    Remote Chassis ID Subtype: Mac address (4)
    Remote Chassis ID:  4c:76:25:f4:ab:01
    Remote Port Subtype:  Interface name (5)
    Remote Port ID:  fortyGigE 1/2/8/1
    Local Port ID: TenGigabitEthernet 1/1
    Locally assigned remote Neighbor Index: 1
    Remote TTL:  300
    Information valid for next 201 seconds
    Time since last information change of this neighbor:  00:01:39
    UnknownTLVList:
    OrgUnknownTLVList:
         ((00-01-66),127,  4) ((00-01-66),126,  4) ((00-01-66),125,  4) ((00-01-66),124,  4) ((00-01-66),123,  4)
         ((00-01-66),122,  4) ((00-01-66),121,  4) ((00-01-66),120,  4) ((00-01-66),119,  4) ((00-01-66),118,  4)
   ---------------------------------------------------------------------------

    Remote Chassis ID Subtype: Mac address (4)
    Remote Chassis ID:  4c:76:25:f4:ab:02
    Remote Port Subtype:  Interface name (5)
    Remote Port ID:  fortyGigE 1/2/8/1
    Local Port ID: TenGigabitEthernet 1/1
    Locally assigned remote Neighbor Index: 2
    Remote TTL:  300
    Information valid for next 201 seconds
    Time since last information change of this neighbor:  00:01:39
    UnknownTLVList:
    OrgUnknownTLVList:
         ((00-01-66),127,  4) ((00-01-66),126,  4) ((00-01-66),125,  4) ((00-01-66),124,  4) ((00-01-66),123,  4)
         ((00-01-66),122,  4) ((00-01-66),121,  4) ((00-01-66),120,  4) ((00-01-66),119,  4) ((00-01-66),118,  4)
   ---------------------------------------------------------------------------

    Remote Chassis ID Subtype: Mac address (4)
    Remote Chassis ID:  4c:76:25:f4:ab:03
    Remote Port Subtype:  Interface name (5)
    Remote Port ID:  fortyGigE 1/2/8/1
    Local Port ID: TenGigabitEthernet 1/1
    Locally assigned remote Neighbor Index: 3
    Remote TTL:  300
    Information valid for next 199 seconds
    Time since last information change of this neighbor:  00:01:41
    UnknownTLVList:
    OrgUnknownTLVList:
         ((00-01-66),127,  4) ((00-01-66),126,  4) ((00-01-66),125,  4) ((00-01-66),124,  4) ((00-01-66),123,  4)
         ((00-01-66),122,  4) ((00-01-66),121,  4) ((00-01-66),120,  4) ((00-01-66),119,  4) ((00-01-66),118,  4)
   ---------------------------------------------------------------------------
```

show lldp statistics

Display the LLDP statistical information.

C9000 Series

Syntax `show lldp statistics`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell#show lldp statistics
Total number of neighbors: 300
Last table change time   :   Mon Oct 02 16:00:52 2006
Number of Table Inserts  :   1621
Number of Table Deletes  :   200
Number of Table Drops    :   0
Number of Table Age Outs :   400
Dell#
```

show management-interface

Display LLDP management interface configuration information.

C9000 Series

Syntax `show management-interface`

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the Z9000 and S4810.

show running-config lldp

Display the current global LLDP configuration.

C9000 Series

Syntax `show running-config lldp`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S8420T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell#show running-config lldp
!
protocol lldp
  advertise dot1-tlv port-protocol-vlan-id port-vlan-id
  advertise dot3-tlv max-frame-size
  advertise management-tlv system-capabilities system-description
  hello 15
  multiplier 3
  no disable
Dell#
```

snmp-notification-interval

Used to configure the value for the lldp notification interval, to throttle lldp notification messages.

Syntax `[no] snmp-notification-interval [seconds]`

To disable this feature, use the `no snmp-notification-interval` command.

Parameters

seconds	Enter a value from 5 to 3600 seconds.

Defaults 5 seconds

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(2.5)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6010–ON and Z9100–ON

Usage Information SNMP notification for the changes in the lldp remote entry table is throttled by 5 seconds (default), or the configured time set using this command. If more than one notification message is generated within the configured time, only the first one will be sent and the remaining messages are suppressed.

LLDP-MED Commands

The following are the LLDP-MED (Media Endpoint Discovery) commands.

The Dell Networking OS LLDP-MED commands are an extension of the set of LLDP TLV advertisement commands. The C-Series and S-Series support all commands.

The E-Series generally supports the commands. However, LLDP-MED commands are more useful on the C-Series and the S50V model of the S-Series, because they support Power over Ethernet (PoE) devices.

As defined by ANSI/TIA-1057, LLDP-MED provides organizationally specific TLVs (Type Length Value), so that endpoint devices and network connectivity devices can advertise their characteristics and configuration information. The Organizational Unique Identifier (OUI) for the Telecommunications Industry Association (TIA) is 00-12-BB.

- LLDP-MED Endpoint Device — any device that is on an IEEE 802 LAN network edge, can communicate using IP, and uses the LLDP-MED framework.
- LLDP-MED Network Connectivity Device — any device that provides access to an IEEE 802 LAN to an LLDP-MED endpoint device, and supports IEEE 802.1AB (LLDP) and TIA-1057 (LLDP-MED). The Dell Networking system is an LLDP-MED network connectivity device.

Regarding connected endpoint devices, LLDP-MED provides network connectivity devices with the ability to:

- manage inventory
- manage Power over Ethernet (POE)
- identify physical location
- identify network policy

advertise med guest-voice

To advertise a separate limited voice service for a guest user with their own IP telephony handset or other appliances that support interactive voice services, configure the system.

C9000 Series

Syntax `advertise med guest-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med guest-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority. The range is from 0 to 7.
DSCP_value	Enter the DSCP value. The range is from 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` followed the Layer 2 priority. The range is from 0 to 7.

Defaults Unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands protocol lldp (Configuration) — enables LLDP globally.

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med guest-voice-signaling

To advertise a separate limited voice service for a guest user when the guest voice control packets use a separate network policy than the voice data, configure the system.

C9000 Series

Syntax `advertise med guest-voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med guest-voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority. The range is from 0 to 7.
DSCP_value	Enter the DSCP value. The range is from 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med location-identification

To advertise a location identifier, configure the system.

C9000 Series

Syntax `advertise med location-identification {coordinate-based value | civic-based value | ecs-elin value}`

To return to the default, use the `no advertise med location-identification {coordinate-based value | civic-based value | ecs-elin value}` command.

Parameters

coordinate-based *value*	Enter the keywords `coordinate-based` then the coordinated based location in hexadecimal value of 16 bytes.
civic-based *value*	Enter the keywords `civic-based` then the civic based location in hexadecimal format. The range is from 6 to 255 bytes.
ecs-elin *value*	Enter the keywords `ecs-elin` then the Emergency Call Service (ecs) Emergency Location Identification Number (elin) numeric location string. The range is from 10 to 25 characters.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Usage Information

- ECS — Emergency call service such as defined by TIA or the national emergency numbering association (NENA)
- ELIN — Emergency location identification number, a valid North America Numbering Plan format telephone number supplied for ECS purposes.

Related Commands debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med power-via-mdi

Configure the system to advertise the IEEE 802.1ab extended power via MDI TLV.

C9000 Series

Syntax `[no] advertise med power-via-mdi`

To return to the default, use the `no advertise med power-via-mdi` command.

Defaults unconfigured.

Command Modes

- LLDP CONFIGURATION (conf-lldp)
- INTERFACE LLDP CONFIGURATION (conf-if-*interface*-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.

Usage Information Advertise extended power via MDI TLVs to all ports that are connected to the 802.1ab powered endpoint devices.

When the `advertise med power-via-mdi` command is enabled in CONFIGURATION mode, advertisement is enabled for all the interfaces in a system. To enable advertisement for a specific interface, configure the command in INTERFACE configuration mode.

Port extender (PE) processes and advertises LLDP power-via-MDI TLVs when the LLDP advertisement of the TLV is enabled on the PE in class power management mode. Incoming LLDP messages are processed only when the PE is in class power management mode.

Related Commands debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med softphone-voice

To advertise softphone to enable IP telephony on a computer so that the computer can be used as a phone, configure the system.

C9000 Series

Syntax `advertise med softphone-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med softphone-voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med streaming-video

To advertise streaming video services for broadcast or multicast-based video, configure the system. This command does not include video applications that rely on TCP buffering.

C9000 Series

Syntax `advertise med streaming-video {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med streaming-video {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med video-conferencing

To advertise dedicated video conferencing and other similar appliances that support real-time interactive video, configure the system.

C9000 Series

Syntax `advertise med video-conferencing {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med video-conferencing {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.

	DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
	priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med video-signaling

To advertise video control packets that use a separate network policy than video data, configure the system.

C9000 Series

Syntax `advertise med video-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med video-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med voice

To advertise a dedicated IP telephony handset or other appliances supporting interactive voice services, configure the system.

C9000 Series

Syntax `advertise med voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med voice {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults unconfigured.

Command Modes CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

advertise med voice-signaling

To advertise when voice control packets use a separate network policy than voice data, configure the system.

C9000 Series

Syntax

`advertise med voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}`

To return to the default, use the `no advertise med voice-signaling {vlan-id layer2_priority DSCP_value} | {priority-tagged number}` command.

Parameters

vlan-id	Enter the VLAN ID. The range is from 1 to 4094.
layer2_priority	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
DSCP_value	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
priority-tagged *number*	Enter the keywords `priority-tagged` then the Layer 2 priority. The range is from 0 to 7.

Defaults

unconfigured.

Command Modes

CONFIGURATION (conf-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series and E-Series.

Related Commands

debug lldp interface — debugs LLDP.

show lldp neighbors — displays the LLDP neighbors.

show running-config lldp — displays the LLDP running configuration.

33

Multicast

The multicast commands are supported by Dell Networking operating system.

This chapter contains the following sections:

- IPv4 Multicast Commands

NOTE: Dell Networking OS supports Multicast routing only on default VRFs .

Topics:

- IPv4 Multicast Commands
- IPv6 Multicast Commands

IPv4 Multicast Commands

The following section contains the IPv4 multicast commands.

clear ip mroute

Clear learned multicast routes on the multicast forwarding table. To clear the protocol-independent multicast (PIM) tree information base, use the `clear ip pim tib` command.

C9000 Series

Syntax `clear ip mroute {group-address [source-address] | * | snooping}`

Parameters

group-address ***[source-address]***	Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
*****	Enter * to clear all multicast routes.
snooping	Enter the keyword `snooping` to delete multicast snooping route table entries.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.(0.0)	Added support for keyword `snooping` on the Z9000, S4810, and S4820T.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series.
E-Series legacy command	

Related Commands show ip pim tib — shows the PIM tree information base.

mtrace

Trace a multicast route from the source to the receiver.

Syntax

```
mtrace [vrf vrf-name] {source-address/hostname} [destination-address/hostname]
[group-address/hostname]
```

Parameters

vrf *vrf-name*	Enter the keyword `vrf` followed by the name of the VRF. If VRF name is not mentioned, the default VRF will be used. Mtrace is not supported for management VRF.
source-address/ hostname	Enter the source IP address in dotted decimal format (A.B.C.D). This is a unicast address of the beginning of the path to be traced.
destination-address/ hostname	Enter the destination (receiver) IP address in dotted decimal format (A.B.C.D). If omitted, the mtrace starts from the system at which the command is typed.
group-address/ hostnamae	Enter the multicast group address in dotted decimal format (A.B.C.D). If group address is not given then software shall invokes a weak mtrace. A weak mtrace is one that follows the RPF path to the source, regardless of whether any router along the path has multicast routing table state

Command Modes EXEC Privilege

Command History

Version	Description
9.11.0.0	Re-introduced the mtrace command on the Dell Networking OS.
7.5.1.0	Expanded to support originator.
7.4.1.0	Expanded to support the intermediate (transit) router.

Usage Information

Mtrace is an IGMP based protocol that provides a multicast trace route facility and is implemented according to the IETF draft "A *trace route* facility for IP Multicast" (draft-fenner-traceroute-ipm-01.txt). Dell Networking OS supports the Mtrace client and transit functionality.

As an Mtrace client, Dell Networking OS transmits Mtrace queries, receives, parses, and prints out the details in the response packet received.

A transit or intermediate router, forwards mtrace requests to the RPF neighbor after appending its response block to the packet. In case it is the first hop router, it sends a response.

As an Mtrace transit or intermediate router, Dell Networking OS returns the response to Mtrace queries. After receiving the Mtrace request, Dell Networking OS computes the RPF neighbor for the source, fills in the request and the forwards the request to the RPF neighbor.

Example

```
R1>mtrace 103.103.103.3 1.1.1.1 226.0.0.3
Type Ctrl-C to abort.

Querying reverse path for source 103.103.103.3 to destination 1.1.1.1 via
group 226.0.0.3
From source (?) to destination (?)

-----------------------------------------------------------------
|Hop|    OIF IP     |Proto| Forwarding Code |Source Network/Mask|
-----------------------------------------------------------------
  0  1.1.1.1          -->    Destination
 -1  1.1.1.1          PIM   Reached RP/Core   103.103.103.0/24
 -2  101.101.101.102  PIM       -             103.103.103.0/24
 -3  2.2.2.1          PIM       -             103.103.103.0/24
 -4  103.103.103.3    -->    Source
-----------------------------------------------------------------
```

The mtrace command traverses the path of the response data block in the reverse direction of the multicast data traffic. The mtrace command traverses the reverse path to the source from the destination. As a result, the tabular output of the mtrace command displays the destination details in the first row, followed by the RPF router details along the path in the consequent rows, and finally the source details in the last row. The tabular output contains the following columns:

- Hop — a hop number(counted negatively to indicate reverse-path)
- OIF IP — outgoing interface address
- Proto — multicast routing protocol
- Forwarding code — error code as present in the response blocks
- Source Network/Mask — source mask

ip mroute

Assign a static mroute.

C9000 Series

Syntax

`ip mroute` *`destination mask`* `{`*`ip-address`* `| null 0| {{bgp| ospf}` *`process-id`* `| isis | rip | static}` `{`*`ip-address`* `| tag | null 0}} [distance]`

To delete a specific static mroute, use the `no ip mroute` *`destination mask`* `{`*`ip-address`* `| null 0| {{bgp| ospf}` *`process-id`* `| isis | rip | static}` `{`*`ip-address`* `| tag | null 0}} [distance]` command.

To delete all mroutes matching a certain mroute, use the `no ip mroute` *`destination mask`* command.

Parameters

destination	Enter the IP address in dotted decimal format of the destination device.
mask	Enter the mask in slash prefix formation (/x) or in dotted decimal format.
null 0	(OPTIONAL) Enter the keyword `null` then zero (0).
[*protocol* [*process-id* | *tag*] *ip-address*]	(OPTIONAL) Enter one of the routing protocols: • Enter the BGP as-number then the IP address in dotted decimal format of the reverse path forwarding (RPF) neighbor. The range is from 1 to 65535. • Enter the OSPF process identification number then the IP address in dotted decimal format of the RPF neighbor. the range is from 1 to 65535.

- Enter the IS-IS alphanumeric tag string then the IP address in dotted decimal format of the RPF neighbor.
- Enter the RIP IP address in dotted decimal format of the RPF neighbor.

static *ip-address*	(OPTIONAL) Enter the Static IP address in dotted decimal format of the RPF neighbor.
ip-address	(OPTIONAL) Enter the IP address in dotted decimal format of the RPF neighbor.
distance	(OPTIONAL) Enter a number as the distance metric assigned to the mroute. The range is from 0 to 255.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
E-Series legacy command	

Related Commands show ip mroute — displays the routing table.

ip multicast-limit

To limit the number of multicast entries on the system, use this feature.

C9000 Series

Syntax `ip multicast-limit [vrf vrf-name] limit`

Parameters

limit	Enter the desired maximum number of multicast entries on the system. The range is from 1 to 16000.

Defaults The default is **4000**.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information

This feature allows you to limit the number of multicast entries on the system. This number is the total of all the multicast entries on all line cards in the system. On each line card, the multicast module only installs the maximum number of entries, depending on the configured CAM profile.

To store multicast routes, use the IN-L3-McastFib CAM partition. It is a separate hardware limit that exists per port-pipe. This hardware space limitation can supersede any software-configured limit. The opposite is also true, the CAM partition might not be exhausted at the time the system-wide route limit set by the `ip multicast-limit` command is reached.

Related Commands

show ip igmp groups — shows the IGMP groups.

ip multicast-routing

Enable IP multicast forwarding.

C9000 Series

Syntax

```
ip multicast-routing
```

To disable multicast forwarding, use the `no ip multicast-routing` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

Version	Description
E-Series legacy command	

Usage Information After you enable multicast, you can enable IGMP and PIM on an interface. In INTERFACE mode, enter the `ip pim sparse-mode` command to enable IGMP and PIM on the interface.

Related Commands ip pim sparse-mode — enables IGMP and PIM on an interface.

show ip multicast-cam

Display the content addressable memory (CAM) size and the portions allocated for IP multicast traffic.

Syntax `show ip multicast-cam linecard slot-id port-set port-pipe`

Parameters

linecard *slot-id*	Enter the keyword `linecard` with a slot number to select the line card for which to gather information. The range of Z9500 slot IDs is from 0 to 2.
port-set *port-pipe*	Enter the keyword `port-set` with a port-pipe number to select the port pipe for which to gather information. The range of port pipes is from 0 to 3.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

Version	Description
E-Series legacy command	

Example

```
show ip multicast-cam stack-unit 1 port 0
Vrf Id       Group Address     Source Address   Vlan Id     IPMC index     L2 Ports       L3 Ports
--------    ---------------   ---------------   -------    ------------   ------------
------------
0             224.1.1.1         0.0.0.0           1000      1             Te 0/3,         Te 0/10,
0             224.1.1.2         0.0.0.0           1000      1             Te 0/3,         Te 0/10,
0             224.1.1.1         165.13.34.5       2000      2             Te 0/5,         Te 0/11,
```

show ip mroute

View the multicast routing table.

C9000 Series

Syntax

```
show ip mroute [static | group-address [source-address] | count | snooping
[vlan vlan-id] [group-address [source-address]] | summary | vlt [group-address
[source-address] | count]
```

Parameters

static	(OPTIONAL) Enter the keyword `static` to view static multicast routes.
group-address [*source-address*]	(OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.
count	(OPTIONAL) Enter the keyword `count` to view the number of multicast routes and packets.
snooping [vlan *vlan-id*] [*group-address* [*source-address*]]	Enter the keyword `snooping` to display information on the multicast routes PIM-SM snooping discovers. Enter a VLAN ID to limit the information displayed to the multicast routes PIM-SM snooping discovers on a specified VLAN. The VLAN ID range is from 1 to 4094. Enter a multicast group address and, optionally, a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes PIM-SM snooping discovers for a specified multicast group and source.
summary	(OPTIONAL) Enter the keyword `summary` to view a summary of all routes.
vlt	(OPTIONAL) Enter the keyword `vlt` to view multicast routes with a spanned incoming interface. Enter a multicast group address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes for a specified multicast group and optionally a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed for a specified multicast source. Enter the keyword `count` to display the total number of multicast routes with the spanned IIF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
9.2.(0.0)	Added support for keyword `vlt` to the Z9000, S4810, and S4820T.
8.4.1.1	Support for the keyword `snooping` and the optional `vlan vlan-id`, `group-address`, and `source-address` parameters were added on E-Series ExaScale.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Example (Static)

```
Dell#show ip mroute static

Mroute: 23.23.23.0/24, interface: Lo 2
Protocol: static, distance: 0, route-map: none, last change: 00:00:23
```

Example (Snooping)

```
 Dell#show ip mroute snooping

IPv4 Multicast Snooping Table

(*, 224.0.0.0), uptime 17:46:23
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/13

(*, 225.1.2.1), uptime 00:04:16
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/11
    GigabitEthernet 4/13

(165.87.1.7, 225.1.2.1), uptime 00:03:17
  Incoming vlan: Vlan 2
  Outgoing interface list:
    GigabitEthernet 4/11
    GigabitEthernet 4/13
    GigabitEthernet 4/20
```

Example (VLT)

```
Dell#show ip mroute vlt
IP Multicast Routing Table
Flags: S - Synced
(*, 225.1.1.1), uptime 00:39:33 flags: S
Incoming interface: Vlan 10
Spanned outgoing interface list:
 Vlan 20 (S)
Vlan 30

(50.1.1.2, 225.1.1.1), uptime 00:39:33 flags: S
Incoming interface: Vlan 10
```

```
Spanned outgoing interface list:
Vlan 20 (S)
```

Usage Information The following describes the `show ip mroute` command shown in the following example.

Field	Description
(S, G)	Displays the forwarding entry in the multicast route table.
uptime	Displays the amount of time the entry has been in the multicast forwarding table.
Incoming interface	Displays the reverse path forwarding (RPF) information towards the source for (S,G) entries and the RP for (*,G) entries.
Outgoing interface list:	Lists the interfaces that meet one of the following: • a directly connected member of the Group • statically configured member of the Group • received a (*,G) or (S,G) Join message

Example

show ip rpf

View reverse path forwarding.

C9000 Series

Syntax `show ip rpf`

Command Modes
- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
E-Series legacy command	

Usage Information Network administrators use static mroutes to control the reach-ability of the multicast sources. If a PIM-registered multicast source is reachable using static mroute as well as unicast route, the distance of each route is examined and the route with shorter distance is the one the PIM selects for reach-ability.

NOTE: The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.

Example

```
Dell#show ip rpf
RPF information for 10.10.10.9
  RPF interface: Gi 3/4
  RPF neighbor: 165.87.31.4
  RPF route/mask: 10.10.10.9/255.255.255.255
  RPF type: unicast
```

IPv6 Multicast Commands

The following section contains the IPv6 multicast commands.

clear ipv6 mroute

Clear learned multicast routes on the multicast forwarding table.

Syntax

```
clear ipv6 mroute [vrf vrf-name] {group-address [source-address] | *}
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**
group-address [*source-address*]	Enter the multicast group address and source address (if desired), in dotted decimal format, to clear information on a specific group.
*	Enter * to clear all multicast routes.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11.3.0	Introduced on the C9000, S3048–ON, S3100, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON and Z9100–ON.

Related Commands

- show ip pim tib — show the PIM tree information base.

ipv6 multicast-routing

Enables IPv6 multicast forwarding.

Syntax

```
ipv6 multicast-routing [vrf vrf-name]
```

To disable multicast forwarding, use the `no ipv6 multicast-routing [vrf vrf-name]` command.

Defaults

Disabled.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to enable IP multicast forwarding on that VRF.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

9.11.3.0	Introduced on the C9000, S3048–ON, S3100, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON and Z9100–ON.

Usage Information After you enable multicast, you can enable IGMP and PIM on an interface. In INTERFACE mode, enter the `ip pim sparse-mode` command to enable IGMP and PIM on the interface.

Related Commands

- ip pim sparse-mode — enable IGMP and PIM on an interface.

show ipv6 mroute

View the IPv6 multicast routing table.

Syntax

```
show ipv6 mroute [vrf vrf-name] [static | group-address [source-address] |
count] | summary | vlt [group-address [source-address] | count]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**
static	(OPTIONAL) Enter the keyword `static` to view static multicast routes.
group-address [*source-address*]	(OPTIONAL) Enter the multicast group-address to view only routes associated with that group. Enter the source-address to view routes with that group-address and source-address.
count	(OPTIONAL) Enter the keyword `count` to view the number of multicast routes and packets.
summary	(OPTIONAL) Enter the keyword `summary` to view a summary of all routes.
vlt	(OPTIONAL) Enter the keyword `vlt` to view multicast routes with a spanned incoming interface. Enter a multicast group address in dotted decimal format (A.B.C.D) to limit the information displayed to the multicast routes for a specified multicast group and optionally a source multicast address in dotted decimal format (A.B.C.D) to limit the information displayed for a specified multicast source. Enter the keyword `count` to display the total number of multicast routes with the spanned IIF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

9.11.3.0	Introduced on the C9000, S3048–ON, S3100, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON and Z9100–ON.

Example

```
Dell# show ipv6 mroute

IP Multicast Routing Table

(*, ff0e:225:0:1::1), uptime 18:01:56
  Incoming interface: Null
  Outgoing interface list:
    Vlan 401
    Vlan 1001

(2001:120:3:1::11, ff0e:225:0:1::1), uptime 18:02:03
  Incoming interface: Vlan 401
  Outgoing interface list:
    Vlan 1001

(2001:130:3:1::11, ff0e:225:0:1::1), uptime 18:01:17
  Incoming interface: Vlan 1001
  Outgoing interface list:
    Vlan 401

(2001:140:3:1::11, ff0e:225:0:1::1), uptime 18:01:13
  Incoming interface: Vlan 1001
  Outgoing interface list:
    Vlan 401

Dell#
```

show ipv6 multicast-cam

Display the content addressable memory (CAM) size and the portions allocated for IP multicast traffic.

Syntax

```
show ipv6 multicast-cam [linecard slot-id | port-set port-pipe | stack-unit unit-id]
```

Parameters

linecard *slot-id*	Enter the keyword `linecard` with a slot id to select the line card for which to gather information. The range of slot IDs is from 0 to 2.
port-set *port-pipe*	Enter the keyword `port-set` with a port-pipe number to select the port pipe for which to gather information. The range of port pipes is from 0 to 3.
stack-unit *unit-id*	Enter the keyword `stack-unit` with a unit-id number to select the stack unit for which to gather information.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

9.11.3.0	Introduced on the C9000, S3048–ON, S3100, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON and Z9100–ON.

Example

```
Dell# show ipv6 multicast-cam stack-unit 1 port-set 0

Group Address  : ff0e::228:1:1
Source Address : 400::2
VRF    : 1
VlanId : 4095
IPMC     : 609
L2 Ports :  -
L3 Ports : Te  0/10
```

show ipv6 rpf

View reverse path forwarding.

Syntax `show ipv6 rpf`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11.3.0	Introduced on the C9000, S3048–ON, S3100, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON and Z9100–ON.

Usage Information Network administrators use static mroutes to control the reach-ability of the multicast sources. If a PIM-registered multicast source is reachable using static mroute as well as unicast route, the distance of each route is examined and the route with shorter distance is the one the PIM selects for reach-ability.

NOTE: The default distance of mroutes is zero (0) and is CLI configurable on a per route basis.

Example

34

Multicast Listener Discovery Protocol

The Multicast Listener Discovery (MLD) protocol is used by IPv6 routers to discover multicast listeners on a directly attached link. Similar to the Internet Group Management Protocol (IGMP), which handles multicast group memberships in IPv4 networks, MLD is used for multicast management on IPv6 networks.

Topics:

- clear ipv6 mld groups
- debug ipv6 mld
- ipv6 mld explicit-tracking
- ipv6 mld last-member-query-interval
- ipv6 mld query-interval
- ipv6 mld query-max-resp-time
- ipv6 mld version
- show ipv6 mld groups
- show ipv6 mld interface
- MLD Snooping

clear ipv6 mld groups

Clear entries from the group cache table.

Syntax

```
clear ipv6 mld [vrf vrf-name] groups [interface | group-address]
```

Parameters

vrf *vrf-name*	(Optional) Enter the keyword `vrf` followed by the name of the VRF.
interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
group-address	(OPTIONAL) Enter the group address in the following format: x:x:x:x::x. The :: notation specifies successive hexadecimal fields of zero.

Defaults None.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(3.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

debug ipv6 mld

Enable debugging on IPv6 MLD packets.

Syntax

`debug ipv6 mld [vrf vrf-name] {group-address | interface}`

To turn off debugging, use the `no debug ipv6 mld {group-address | interface}` command.

Parameters

vrf *vrf-name*	(Optional) Enter the keyword `vrf` followed by the name of the VRF.
group-address	(OPTIONAL) Enter the multicast group address in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.
interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Defaults Disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(3.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld explicit-tracking

Enable MLD explicit tracking receivers.

Syntax

`ipv6 mld explicit-tracking`

To disable explicit tracking, use the `no ipv6 mld explicit-tracking` command.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(3.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld last-member-query-interval

Change the MAX Response Time inserted into the Group-Specific Queries sent in response to a Leave Group messages. This interval is also the interval between Group-Specific Query messages.

Syntax

```
ipv6 mld last-member-query-interval {milliseconds}
```

To return to the default, use the `no ipv6 mld last-member-query-interval {milliseconds}` command.

Parameters

milliseconds	Enter the last member query interval in milliseconds. The range is from 100 to 65535.

Defaults 1000 milliseconds.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(3.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld query-interval

Change the transmission frequency of the MLD host.

Syntax

```
ipv6 mld query-interval [seconds]
```

To return to the default interval, use the `no ipv6 mld query-interval` command.

Parameters

seconds	Enter the interval in seconds. The range is from 1 to 18000.

Defaults 60 seconds.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(3.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld query-max-resp-time

Set the maximum query response time advertised in the general queries.

Syntax

```
ipv6 mld query-max-resp-time {seconds}
```

To return to the default, use the `no ipv6 mld query-max-resp-time` command.

Parameters

seconds	Enter the interval in seconds. The range is from 1 to 25.

Defaults

10 seconds.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(3.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld version

Configure the MLD version on the system.

Syntax

```
ipv6 mld version {1 | 2}
```

Defaults

MLD version 2

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F–ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

Usage Information

The `ipv6 mld version` command is applicable for MLD snooping-enabled interfaces.

Example

The following is a sample configuration wherein MLD version 1 is selected on the system.

```
interface Vlan 61
 ip vrf forwarding red
  ipv6 address 61::9/64
 ipv6 ospf 2 area 0
 untagged TenGigabitEthernet 2/18
  ipv6 pim sparse-mode
 ipv6 mld version 1
 no shutdown
```

show ipv6 mld groups

View the configured MDL groups.

Syntax `show ipv6 mld [vrf vrf-name] groups [detail] [group-address] [interface interface [detail]]`

Parameters

vrf *vrf-name*	(Optional) Enter the keyword `vrf` followed by the name of the VRF.
group-address	Enter the group address for which you want to display information.
interface *interface*	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
detail	View detailed group information.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(3.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

Example

```
Dell#show ipv6 mld groups
Total Number of Groups: 1
MLD Connected Group Membership
Group Address    Interface    Mode     Uptime    Expires     Last Reporter
 Ff08::12         Vlan 10     MLDv2   00:00:12  00:02:05     1::2
```

show ipv6 mld interface

View the configured MLD interfaces.

Syntax `show ipv6 mld [vrf vrf-name] interface [interface]`

Parameters

vrf *vrf-name*	(Optional) Enter the keyword `vrf` followed by the name of the VRF.
interface *interface*	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.11(3.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

Example

```
Dell#show ipv6 mld interface vlan 20
 Vlan 20 is up, line protocol is up
 Inbound MLD access group is not set
 Internet address is fe80::92b1:1cff:fef4:9b63/64
 MLD is enabled on interface
 MLD query interval is 60 seconds
 MLD querier timeout is 125 seconds
 MLD max query response time is 10 seconds
 MLD last member query response interval is 1000 ms
 MLD immediate-leave is enabled for all groups
 MLD activity: 0 joins
 MLD querying router is 35::1 (this system)
 MLD version is 2
```

MLD Snooping

MLD snooping allows the switch to examine the MLD packets and forwards the decision based on their content. You can configure MLD snooping in subnets that receive MLD queries from either MLD or the MLD snooping querier. MLD snooping limits the IPv6 multicast traffic at Layer 2 by configuring Layer 2 LAN ports and dynamically forwards the IPv6 multicast traffic to the ports that want to receive it. Hosts join IPv6 multicast groups either by sending an unsolicited MLD report or by sending an MLD report in response to a general query from an IPv6 multicast router (the switch forwards general queries from IPv6 multicast routers to all the ports in a VLAN). The switch snoops these reports and in response to a snooped MLD report, the switch creates an entry in its forwarding table for the VLAN on which the report was received. When the other hosts that are interested in this multicast traffic send MLD reports, the switch snoops their report and adds them to the existing forwarding table entry. The switch creates only one entry per VLAN in the forwarding table for each multicast group, for which it snoops an MLD report.

clear ipv6 mld snooping groups

Clear entries from the group cache table.

Syntax

```
clear ipv6 mld snooping groups [interface | group-address]
```

Parameters

interface	Enter the following keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
group-address	(OPTIONAL) Enter the group address in the following format: x:x:x:x::x. The :: notation specifies successive hexadecimal fields of zero.

Defaults

None.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

debug ipv6 mld snooping

Enable debugging on IPv6 MLD snooping packets.

Syntax `debug ipv6 mld {group-address | interface}`

To turn off debugging, use the `no debug ipv6 mld {group-address | interface}` command.

Parameters

group-address (OPTIONAL) Enter the multicast group address in the x:x:x:x::x format. The :: notation specifies successive hexadecimal fields of zero.

interface Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Defaults Disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld snooping

Enable MLD snooping on a VLAN.

Syntax `ipv6 mld snooping`

To disable MLD snooping, use the `no ipv6 mld snooping` command.

Defaults Enabled on all VLAN interfaces.

Command Modes INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld snooping enable

Enable MLD snooping on the switch globally.

Syntax

```
ipv6 mld snooping enable
```

To disable MLD snooping, use the `no ipv6 mld snooping enable` command.

Defaults

Enabled on all VLAN interfaces.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld snooping explicit-tracking

Enable explicit MLD snooping tracking on an interface.

Syntax

```
ipv6 mld snooping explicit-tracking
```

To disable MLD snooping explicit tracking, use the `no ipv6 mld snooping explicit-tracking` command.

Defaults

Disabled.

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld snooping mrouter

Configure a Layer 2 port as a multicast router port.

Syntax `ipv6 mld snooping mrouter interface {interface` *`interface`*`}`

Parameters

interface	Enter the keyword `interface`to indicate the next-hop interface to the multicast router.
interface	Enter one of the following keywords and the interface information: • For a null interface, enter the keyword `null` then the slot/port information. The Null interface number is 0. • For the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094. • For a port channel interface, enter the keywords `port-channel` then a number.

Defaults None.

Command Modes INTERFACE VLAN

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

ipv6 mld snooping querier

Enable the MLD querier processing for the VLAN interface.

Syntax `ipv6 mld snooping querier`

To disable the querier feature, use the `no ipv6 mld snooping querier` command.

Defaults Disabled

Command Modes INTERFACE VLAN

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

show ipv6 mld snooping groups

Display the IPv6 MLD snooping group information.

Syntax

```
show ipv6 mld snooping groups [group address] [summary] [interface interface [detail]]
```

Parameters

group-address	(Optional) Enter the multicast group addresss in the X:X:X:X::X format. The :: notation specifies successive hexadecimal fields of zero.
summary	(OPTIONAL) Enter the keyword `summary` to display a summary of groups.
interface *interface*	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.
detail	View detailed group information.

Defaults None.

Command Modes EXEC

EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

Example

```
Dell EMC#show ipv6 mld snooping groups
Total Number of Groups: 1
Channel ::/ff0e::225:1:1:1, interface Vlan 10
  Uptime 11:24:49 , Last join time 00:00:15
  Expires in 00:01:54
  Ports : Po 1
Dell EMC#
```

show ipv6 mld snooping interface

View the configured MLD snooping interfaces.

Syntax

```
show ipv6 mld snooping interface [interface]
```

Parameters

interface *interface* Enter the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a VLAN, enter the keyword `vlan` followed by a number from 1 to 4094.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

Example

```
DellEMC#show ipv6 mld snooping interface vlan 10
Vlan 10 is up, line protocol is up
  Interface address is fe80::3617:ebff:fe30:2482/64
  MLD protocol processing disabled
  Current MLD snooping version is 2
  MLD snooping is enabled on this interface
  MLD snooping querier is disabled and is currently inactive
  MLD snooping last member query response interval is 1000 ms
  MLD snooping explicit tracking is disabled
```

show ipv6 mld snooping mrouter

Display information on the MLD snooping router.

Syntax `show ipv6 mld snooping mrouter [vlan]`

Parameters

VLAN (OPTIONAL) Enter the keyword `VLAN` then the VLAN number to display the information on that specific VLAN. The VLAN range is from 1 to 4094.

Defaults None.

Command Modes EXEC

EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, S3100, and C9010.

Example

```
Dell#show ipv6 mld snooping mrouter
Interface Ports (* - Dynamic)
```

```
Vlan 2 Gi 1/18
Dell#
```

35

Multicast Source Discovery Protocol (MSDP)

Multicast source discovery protocol (MSDP) connects multiple PIM Sparse-Mode (PIM-SM) domains together.

MSDP peers connect using TCP port 639. Peers send keepalives every 60 seconds. A peer connection is reset after 75 seconds if no MSDP packets are received. MSDP connections are parallel with MBGP connections.

Topics:

- clear ip msdp peer
- clear ip msdp sa-cache
- clear ip msdp statistic
- debug ip msdp
- ip msdp cache-rejected-sa
- ip msdp default-peer
- ip msdp log-adjacency-changes
- ip msdp mesh-group
- ip msdp originator-id
- ip msdp peer
- ip msdp redistribute
- ip msdp sa-filter
- ip msdp sa-limit
- ip msdp shutdown
- ip multicast-msdp
- show ip msdp
- show ip msdp sa-cache rejected-sa

clear ip msdp peer

Reset the TCP connection to the peer and clear all the peer statistics.

C9000 Series

Syntax	`clear ip msdp peer {peer address}`	
Parameters	**peer address**	Enter the peer address in a dotted decimal format (A.B.C.D.)
Defaults	Not configured.	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.	

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
6.2.1.1	Introduced

clear ip msdp sa-cache

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

C9000 Series

Syntax `clear ip msdp sa-cache [group-address | rejected-sa | local]`

Parameters

group-address	Enter the group IP address in dotted decimal format (A.B.C.D.).
rejected-sa	Enter the keywords `rejected-sa` to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.
local	Enter the keyword `local` to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.

Defaults Without any options, this command clears the entire source-active cache.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.8.1.0	Added the `local` option.
7.7.1.0	Added the `rejected-sa` option.

Version	Description
6.2.1.1	Introduced

clear ip msdp statistic

Clears the entire source-active cache, the source-active entries of a particular multicast group, rejected, or local source-active entries.

C9000 Series

Syntax `clear ip msdp sa-cache [group-address | rejected-sa | local]`

Parameters

group-address	Enter the group IP address in dotted decimal format (A.B.C.D.).
rejected-sa	Enter the keyword `rejected-sa` to clear the cache source-active entries that are rejected because the RPF check failed, an SA filter or limit is configured, the RP or MSDP peer is unreachable, or because of a format error.
local	Enter the keyword `local` to clear out local PIM advertised entries. It applies the redistribute filter (if present) while adding the local PIM SA entries to the SA cache.

Defaults Without any options, this command clears the entire source-active cache.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.8.1.0	Added the `local` option.
7.7.1.0	Added the `rejected-sa` option.
6.2.1.1	Introduced

debug ip msdp

Turn on MSDP debugging.

C9000 Series

Syntax

`debug ip msdp {event` *`peer address`* `| packet` *`peer address`* `| pim}`

To turn debugging off, use the `no debug ip msdp {event` *`peer address`* `| packet` *`peer address`* `| pim}` command.

Parameters

event ***peer address***	Enter the keyword `event` then the peer address in a dotted decimal format (A.B.C.D.).
packet ***peer address***	Enter the keyword `packet` then the peer address in a dotted decimal format (A.B.C.D.).
pim	Enter the keyword `pim` to debug advertisement from PIM.

Defaults

Not configured.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced

ip msdp cache-rejected-sa

Enable an MSDP cache for the rejected source-active entries.

C9000 Series

Syntax

`ip msdp cache-rejected-sa {`*`number`*`}`

To clear the MSDP rejected source-active entries, use the `no ip msdp cache-rejected-sa {`*`number`*`}` command then the `ip msdp cache-rejected-sa {`*`number`*`}` command.

Parameters

number	Enter the number of rejected SA entries to cache. The range is from 0 to 32766.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.4.1.0	Introduced

Related Commands show ip msdp sa-cache rejected-sa

ip msdp default-peer

Define a default peer from which to accept all source-active (SA) messages.

C9000 Series

Syntax `ip msdp default-peer` *`peer address`* `[list` *`name`*`]`

To remove the default peer, use the `no ip msdp default-peer {`*`peer address`*`} list` *`name`* command.

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.)
list *name*	Enter the keywords `list name` and specify a standard access list that contains the RP address that should be treated as the default peer. If no access list is specified, then all SAs from the peer are accepted.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added the `list` option and removed the `prefix-list` option.
7.4.1.0	Introduced

Usage Information If a list is not specified, all SA messages received from the default peer are accepted. You can enter multiple `default peer` commands.

ip msdp log-adjacency-changes

Enable logging of MSDP adjacency changes.

C9000 Series

Syntax `ip msdp log-adjacency-changes`

To disable logging, use the `no ip msdp log-adjacency-changes` command.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced

ip msdp mesh-group

To be a member of a mesh group, configure a peer.

C9000 Series

Syntax

```
ip msdp mesh-group {name} {peer address}
```

To remove the peer from a mesh group, use the `no ip msdp mesh-group {name} {peer address}` command.

Parameters

name	Enter a string of up to 16 characters long for as the mesh group name.
peer address	Enter the peer address in a dotted decimal format (A.B.C.D.).

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced

Usage Information An MSDP mesh group is a mechanism for reducing SA flooding, typically in an intra-domain setting. When some subset of a domain's MSDP speakers are fully meshed, they can be configured into a mesh-group. If member X of a mesh-group receives a SA message from an MSDP peer that is also a member of the mesh-group, member X accepts the SA message and forwards it to all of its peers that are not part of the mesh-group. However, member X cannot forward the SA message to other members of the mesh-group.

ip msdp originator-id

Configure the MSDP Originator ID.

C9000 Series

Syntax

```
ip msdp originator-id {interface}
```

To remove the originator-id, use the `no ip msdp originator-id {interface}` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
6.2.1.1	Introduced

ip msdp peer

Configure an MSDP peer.

C9000 Series

Syntax `ip msdp peer peer address [connect-source] [description] [sa-limit number]`

To remove the MSDP peer, use the `no ip msdp peer peer address [connect-source interface] [description name] [sa-limit number]` command.

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.).
connect-source *interface*	Enter the keywords `connect-source` then one of the interfaces and slot/port or number information:

- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

description name	(OPTIONAL) Enter the keyword *description* then a description name (maximum 80 characters) to designate a description for the MSDP peer.
sa-limit *number*	(OPTIONAL) Enter the maximum number of SA entries in SA-cache. The range is from 1 to 500000. The default it **500000**.

Defaults As described in the *Parameters* section.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
7.5.1.0	Added option for SA upper limit and the `description` option.
6.2.1.1	Introduced

Usage Information The `connect-source` option is used to supply a source IP address for the TCP connection. When an interface is specified using the `connect-source` option, the primary configured address on the interface is used.

If the total number of SA messages received from the peer is already larger than the limit when this command is applied, those SA messages continue to be accepted. To enforce the limit in such situation, use the `clear ip msdp peer` command to reset the peer.

Related Commands ip msdp sa-limit — configures the MSDP SA Limit.

clear ip msdp peer — clears the MSDP peer.

show ip msdp — displays the MSDP information.

ip msdp redistribute

Filter local PIM SA entries in the SA cache. SAs which the ACL denies time out and are not refreshed. Until they time out, they continue to reside in the MSDP SA cache.

C9000 Series

Syntax `ip msdp redistribute [list acl-name]`

Parameters

list *acl-name*	lEnter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced

Usage Information Modifications to the ACL do not have an immediate effect on the sa-cache.

To apply the redistribute filter to entries already present in the SA cache, use the `clear ip msdp sa-cache local` command.

ip msdp sa-filter

Permit or deny MSDP source active (SA) messages based on multicast source and/or group from the specified peer.

C9000 Series

Syntax `ip msdp sa-filter {in | out} peer-address list [access-list name]`

Remove this configuration using the `no ip msdp sa-filter {in | out} peer address list [access-list name]` command.

Parameters

in	Enter the keyword `in` to enable incoming SA filtering.
out	Enter the keyword `out` to enable outgoing SA filtering.
peer-address	Enter the peer address of the MSDP peer in a dotted decimal format (A.B.C.D.).
access-list name	Enter the name of an extended ACL that contains permitted SAs. If you do not use this option, all local entries are blocked.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the E-Series.

ip msdp sa-limit

Configure the upper limit of source-active (SA) entries in SA-cache.

C9000 Series

Syntax `ip msdp sa-limit` *`number`*

To return to the default, use the `no ip msdp sa-limit` *`number`* command.

Parameters

number	Enter the maximum number of SA entries in SA-cache. The range is from 0 to 40000.

Defaults **50000**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the E-Series.

Usage Information

The system counts the SA messages originated by itself and those messages received from the MSDP peers. When the total SA messages reach this limit, the subsequent SA messages are dropped (even if they pass RPF checking and policy checking).

If the total number of SA messages is already larger than the limit when this command is applied, those SA messages that are already in the system continue to be accepted. To enforce the limit in such situation, use the `clear ip msdp sa-cache` command.

Related Commands

ip msdp peer — configures the MSDP peer.

clear ip msdp peer — clears the MSDP peer.

show ip msdp — displays the MSDP information

ip msdp shutdown

Administratively shut down a configured MSDP peer.

C9000 Series

Syntax

```
ip msdp shutdown {peer address}
```

Parameters

peer address	Enter the peer address in a dotted decimal format (A.B.C.D.).

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
6.2.1.1	Introduced

ip multicast-msdp

Enable MSDP.

C9000 Series

Syntax `ip multicast-msdp`

To exit MSDP, use the `no ip multicast-msdp` command.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced

show ip msdp

Display the MSDP peer status, SA cache, or peer summary.

C9000 Series

Syntax `show ip msdp {peer peer address | sa-cache | summary}`

Parameters

peer *peer address*	Enter the keyword `peer` then the peer address in a dotted decimal format (A.B.C.D.).
sa-cache	Enter the keywords `sa-cache` to display the Source-Active cache.
summary	Enter the keyword `summary` to display an MSDP peer summary.

Defaults Not configured.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced

Example

```
Dell#show ip msdp peer 100.1.1.1

Peer Addr: 100.1.1.1
  Local Addr: 100.1.1.2(639) Connect Source: none
  State: Established Up/Down Time: 00:00:08
  Timers: KeepAlive 60 sec, Hold time 75 sec
  SourceActive packet count (in/out): 0/0
  SAs learned from this peer: 0
  SA Filtering:
  Input (S,G) filter: none
  Output (S,G) filter: none
Dell#
```

Example (Sa-cache)

```
Dell#show ip msdp sa-cache
MSDP Source-Active Cache - 1 entries
GroupAddr  SourceAddr     RPAddr        LearnedFrom Expire UpTime
224.1.1.1  172.21.220.10  172.21.3.254  172.21.3.254 102  00:02:52
Dell#
```

Example (Summary)

```
Dell#show ip msdp summary
Peer Addr  Local Addr State       Source SA  Up/Down Description
72.30.1.2  72.30.1.1  Established  none 0  00:00:03 peer1
72.30.2.2  72.30.2.1  Established  none 0  00:00:03 peer2
72.30.3.2  72.30.3.1  Established  none 0  00:00:02 test-peer-3
Dell#
```

show ip msdp sa-cache rejected-sa

Display the rejected SAs in the SA cache.

C9000 Series

Syntax

```
show ip msdp sa-cache rejected-sa
```

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.4.1.0	Introduced.

Example

```
Dell#show ip msdp sa-cache rejected-sa
MSDP Rejected SA Cache 200 rejected SAs received, cache-size 1000
UpTime   GroupAddr SourceAddr RPAddr    LearnedFrom Reason
00:00:13 225.1.2.1 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.2 10.1.1.4   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.3 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.4 10.1.1.4   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.5 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.6 10.1.1.4   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.7 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.8 10.1.1.4   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.9 10.1.1.3   110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.10 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.11 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.11 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.12 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.13 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.14 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.15 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.16 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.17 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.18 10.1.1.4  110.1.1.1 13.1.1.2 Rpf-Fail
00:00:13 225.1.2.19 10.1.1.3  110.1.1.1 13.1.1.2 Rpf-Fail
Dell#
```

36

Multiple Spanning Tree Protocol (MSTP)

Multiple spanning tree protocol (MSTP), as implemented by the Dell Networking operating system, conforms to IEEE 802.1s.

Topics:

- debug spanning-tree mstp
- disable
- forward-delay
- hello-time
- max-age
- max-hops
- msti
- name
- protocol spanning-tree mstp
- revision
- show config
- show spanning-tree mst configuration
- show spanning-tree msti
- spanning-tree
- spanning-tree msti
- spanning-tree mstp edge-port
- tc-flush-standard

debug spanning-tree mstp

Enable debugging of the multiple spanning tree protocol and view information on the protocol.

C9000 Series

Syntax `debug spanning-tree mstp [all | bpdu interface {in | out} | events]`

Parameters

all	(OPTIONAL) Enter the keyword all to debug `all` spanning tree operations.
bpdu interface {in | out}	(OPTIONAL) Enter the keyword `bpdu` to debug bridge protocol data units (BPDU). (OPTIONAL) Enter the interface keyword along with the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Optionally, enter an `in` or `out` parameter with the optional interface:

- For Receive, enter the keyword `in`.
- For Transmit, enter the keyword `out`.

events (OPTIONAL) Enter the keyword `events` to debug MSTP events.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell#debug spanning-tree mstp bpdu tengigabitethernet 2/0 ?
in Receive (in)
out Transmit (out)
```

disable

Globally disable the multiple spanning tree protocol on the switch.

C9000 Series

Syntax `disable`

To enable MSTP, enter the `no disable` command.

Defaults disabled.

Command Modes MULTIPLE SPANNING TREE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Related Commands protocol spanning-tree mstp — enters MULTIPLE SPANNING TREE mode.

forward-delay

The amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

C9000 Series

Syntax `forward-delay` *seconds*

To return to the default setting, use the `no forward-delay` command.

Parameters

seconds	Enter the number of seconds the interface waits in the Blocking State and the Learning State before transiting to the Forwarding State. The range is from 4 to 30. The default is **15 seconds**.

Defaults **15 seconds**

Command Modes MULTIPLE SPANNING TREE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Related Commands

max-age — changes the wait time before MSTP refreshes protocol configuration information.

hello-time — changes the time interval between bridge protocol data units (BPDUs).

hello-time

Set the time interval between generation of MSTB bridge protocol data units (BPDUs).

C9000 Series

Syntax

`hello-time` *seconds*

To return to the default value, use the `no hello-time` command.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is **2 seconds**.

Defaults

2 seconds

Command Modes

MULTIPLE SPANNING TREE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Related Commands

forward-delay — the amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

max-age — changes the wait time before MSTP refreshes protocol configuration information.

max-age

To maintain configuration information before refreshing that information, set the time interval for the MSTB.

C9000 Series

Syntax

`max-age seconds`

To return to the default values, use the `no max-age` command.

Parameters

max-age	Enter a number of seconds the system waits before refreshing configuration information. The range is from 6 to 40. The default is **20 seconds**.

Defaults

20 seconds

Command Modes

MULTIPLE SPANNING TREE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Related Commands

forward-delay — the amount of time the interface waits in the Blocking State and the Learning State before transitioning to the Forwarding State.

hello-time — changes the time interval between BPDUs.

max-hops

Configure the maximum hop count.

C9000 Series

Syntax

```
max-hops number
```

To return to the default values, use the `no max-hops` command.

Parameters

range	Enter a number for the maximum hop count. The range is from 1 to 40. The default is **20**.

Defaults

20 hops

Command Modes

MULTIPLE SPANNING TREE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Usage Information

The `max-hops` command is a configuration command that applies to both the IST and all MST instances in the MSTP region. The BPDUs sent out by the root switch set the remaining-hops parameter to the configured value of max-hops. When a switch receives the BPDU, it decrements the received value of the remaining hops and uses the resulting value as remaining-hops in the BPDUs. If the remaining-hops reach zero, the switch discards the BPDU and ages out any information that it holds for the port.

msti

Configure multiple spanning tree instance, bridge priority, and one or multiple VLANs mapped to the MST instance.

C9000 Series

Syntax

```
msti instance {vlan range | bridge-priority priority}
```

To disable mapping or bridge priority, use the `no msti instance {vlan range | bridge-priority priority}` command.

Parameters

msti *instance*	Enter the MSTP iInstance. The range is from zero (0) to 63.
vlan *range*	Enter the keyword `vlan` then the identifier range value. The range is from 1 to 4094.
bridge-priority *priority*	Enter the keywords `bridge-priority` then a value in increments of 4096 as the bridge priority. The range is from zero (0) to 61440. Valid priority values are: 0, 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344, and 61440. All other values are rejected.

Defaults default bridge-priority is **32768**.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Usage Information By default, all VLANs are mapped to MST instance zero (0) unless you use the `vlan range` command to map it to a non-zero instance.

name

The name you assign to the multiple spanning tree region.

C9000 Series

Syntax `name region-name`

To remove the region name, use the `no name` command.

Parameters

region-name	Enter the MST region name. The range is 32 character limit.

Defaults no default name.

Command Modes MULTIPLE SPANNING TREE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Usage Information For two MSTP switches to be within the same MSTP region, the switches must share the same region name (including matching case).

Related Commands msti — maps the VLAN(s) to an MST instance.

revision — assigns the revision number to the MST configuration.

protocol spanning-tree mstp

To enable and configure the multiple spanning tree group, enter MULTIPLE SPANNING TREE mode.

C9000 Series

Syntax `protocol spanning-tree mstp`

To disable the multiple spanning tree group, use the `no protocol spanning-tree mstp` command.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

MSTP is not enabled when you enter MULTIPLE SPANNING TREE mode. To enable MSTP globally on the switch, enter the `no disable` command while in MULTIPLE SPANNING TREE mode.

For more information about the multiple spanning tree protocol, refer to the *Dell Networking OS Configuration Guide*.

Example

```
Dell(conf)#protocol spanning-tree mstp
Dell(config-mstp)#no disable
```

Related Commands

disable — disables multiple spanning tree.

revision

The revision number for the multiple spanning tree configuration.

C9000 Series

Syntax

`revision` *range*

To return to the default values, use the `no revision` command.

Parameters

range	Enter the revision number for the MST configuration. The range is from 0 to 65535. The default is **0**.

Defaults

0

Command Modes

MULTIPLE SPANNING TREE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information For two MSTP switches to be within the same MST region, the switches must share the same revision number.

Related Commands msti — maps the VLAN(s) to an MST instance.

name — assigns the region name to the MST region.

show config

View the current configuration for the mode. Only non-default values are shown.

C9000 Series

Syntax `show config`

Command Modes MULTIPLE SPANNING TREE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

Example

```
Dell(conf-mstp)#show config
!
protocol spanning-tree mstp
  no disable
  name CustomerSvc
  revision 2
  MSTI 10 VLAN 101-105
  max-hops 5
Dell(conf-mstp)#
```

show spanning-tree mst configuration

View the multiple spanning tree configuration.

C9000 Series

Syntax `show spanning-tree mst configuration`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information Enable the multiple spanning tree protocol prior to using this command.

Example

```
Dell#show spanning-tree mst configuration
MST region name: CustomerSvc
Revision: 2
MSTI VID
  10 101-105
Dell#
```

show spanning-tree msti

View the multiple spanning tree instance.

C9000 Series

Syntax `show spanning-tree msti [instance-number [brief]] [guard]`

Parameters

instance-number	(Optional) Enter the multiple spanning tree instance number. The range is from 0 to 63.
brief	(Optional) Enter the keyword `brief` to view a synopsis of the MST instance.
guard	(Optional) Enter the keyword `guard` to display the type of guard enabled on an MSTP interface and the current port state.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Support for the optional keyword `guard` was added on the C-Series, S-Series, and E-Series TeraScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Expanded to display the port error disable state (EDS) loopback BPDU inconsistency causes.

Usage Information

Enable the multiple spanning tree protocol prior to using this command.

Example

```
Dell#show spanning-tree msti 10
MSTI 10 VLANs mapped 101-105

Bridge Identifier has priority 32768, Address 0001.e802.3506
Configured hello time 2, max age 20, forward delay 15, max hops 5
Current root has priority 16384, Address 0001.e800.0a5c
Number of topology changes 0, last change occurred 3058087

Port 82 (TenGigabitEthernet 2/0) is designated Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.82
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 32768, address 0001.e802.35:06
Designated port id is 128.82, designated path cost
Number of transitions to forwarding state 1
BPDU (Mrecords): sent 1109, received 0
The port is not in the portfast mode

Port 88 (TenGigabitEthernet 2/6) is root Forwarding
Port path cost 0, Port priority 128, Port Identifier 128.88
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.88, designated path cost
Number of transitions to forwarding state 4
BPDU (Mrecords): sent 19, received 1103
```

```
The port is not in the portfast mode

Port 89 (TenGigabitEthernet 2/7) is alternate Discarding
Port path cost 0, Port priority 128, Port Identifier 128.89
Designated root has priority 16384, address 0001.e800.0a:5c
Designated bridge has priority 16384, address 0001.e800.0a:5c
Designated port id is 128.89, designated path cost
Number of transitions to forwarding state 3
BPDU (Mrecords): sent 7, received 1103
The port is not in the portfast mode
```

Example (EDS and LBK)

The bold line shows the loopback BPDU inconsistency (LBK_INC).

```
Dell#show spanning-tree msti 0 brief
MSTI 0 VLANs mapped 1-4094

Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root of MSTI 0 (CIST)
Configured hello time 2, max age 20, forward delay 15, max hops 20
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0

Interface                              Designated
Name    PortID   Prio Cost Sts Cost Bridge ID      PortID
-----------------------------------------------------------
Te 0/0  128.257  128  20000 EDS 0 32768 0001.e801.6aa8 128.257

Interface
Name  Role  PortID Prio Cost Sts Cost Link-type Edge Boundary
-----------------------------------------------------------
Te 0/0 ErrDis 128.257  128 20000 EDS 0   P2P       No   No

Dell#show spanning-tree msti 0
MSTI 0 VLANs mapped 1-4094

Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 20
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max hops 20
We are the root of MSTI 0 (CIST)
Current root has priority 32768, Address 0001.e801.6aa8
CIST regional root ID Priority 32768, Address 0001.e801.6aa8
CIST external path cost 0
Number of topology changes 1, last change occured 00:00:15 ago on Te 0/0

Port 257 (TenGigabitEthernet 0/0) is LBK_INC Discarding
Port path cost 20000, Port priority 128, Port Identifier 128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU (MRecords): sent 21, received 9
The port is not in the Edge port mode
```

Usage Information

The following describes the `show spanning-tree msti 5 guard` command shown in the following example.

Field	Description
Interface Name	MSTP interface.
Instance	MSTP instance.

Field	Description
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

Example (Guard)

```
Dell#show spanning-tree msti 5 guard
Interface
Name    Instance  Sts Guard    type
-----------------------------------
Te 0/1  5         INCON(Root)  Rootguard
Te 0/2  5         FWD          Loopguard
Te 0/3  5         EDS(Shut)    Bpduguard
```

spanning-tree

Enable the multiple spanning tree protocol on the interface.

C9000 Series

Syntax `spanning-tree`

To disable the multiple spanning tree protocol on the interface, use the `no spanning-tree` command.

Parameters

spanning-tree	Enter the keywords `spanning-tree` to enable the MSTP on the interface.

Defaults Enable.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

spanning-tree msti

Configure multiple spanning tree instance cost and priority for an interface.

C9000 Series

Syntax `spanning-tree msti` *instance* {`cost` *cost* | `priority` *priority*}

Parameters

msti *instance*	Enter the keyword `msti` and the MST instance number. The range is from zero (0) to 63.
cost *cost*	(OPTIONAL) Enter the keyword `cost` then the port cost value. The range is from 1 to 200000. The defaults are: • 10-Gigabit Ethernet interface = **2000** • Port Channel interface with one 10 Gigabit Ethernet = **2000** • Port Channel with two 10 Gigabit Ethernet = **1800**
priority *priority*	Enter keyword `priority` then a value in increments of 16 as the priority. The range is from 0 to 240. The default is **128**.

Defaults

- cost = depends on the interface type
- priority = **128**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

spanning-tree mstp edge-port

Configures the interface as an MST edge port and optionally a Bridge Protocol Data Unit (BPDU) guard.

C9000 Series

Syntax `spanning-tree mstp edge-port [bpduguard [shutdown-on-violation]]`

Parameters

mstp edge-port	Enter the keyword `mstp` then the keywords `edge-port` to configure the interface as a Multiple Spanning Tree edge port.
bpduguard	(OPTIONAL) Enter the keyword `portfast` to enable Portfast to move the interface into forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.
shutdown-onviolation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
8.2.1.0	Introduced the hardware `shutdown-on-violation` option.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

Usage Information On an MSTP switch, a port configured as an edge port immediately transitions to the Forwarding state. Only configure ports connected to end-hosts as edge ports. Consider an edge port similar to a port with spanning-tree portfast enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the RPM CPU.

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

C9000 Series

Syntax

`tc-flush-standard`

To disable, use the `no tc-flush-standard` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced

Usage Information

By default, the system implements an optimized flush mechanism for MSTP. This mechanism helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, this `knob` command can be turned on to enable flushing MAC addresses after receiving every topology change notification.

37

Neighbor Discovery Protocol (NDP)

The neighbor discovery protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. NDP defines mechanisms for solving the following problems:

- Router discovery: Hosts can locate routers residing on a link
- Prefix discovery: Hosts can discover address prefixes for the link
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination
- Neighbor unreachability detection (NUD): Determine that a neighbor is no longer reachable on the link.
- Duplicate address detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.

NDP uses the following five ICMPv6 packet types in its implementation:

- Router Solicitation
- Router Advertisement
- Neighbor Solicitation
- Neighbor Advertisement
- Redirect

Topics:

- debug ipv6 nd ra–guard
- device–role
- hop–limit
- ipv6 nd ra–guard attach–policy
- ipv6 nd ra–guard enable
- ipv6 nd ra–guard policy
- managed-config-flag
- match ra
- mtu
- other–config–flag
- reachable–time
- retrans-time
- router–lifetime
- router–preference maximum
- show config
- show ipv6 nd ra–guard policy
- trusted–port

debug ipv6 nd ra–guard

Enable debugging for IPv6 RA guard snooping information.

Syntax

```
debug ipv6 nd ra-guard [interface_type slot/port | count value]
```

Parameters

interface_type slot/port	Enter the one of the following interfaces and slot/port information: • For a port channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
count *value*	Enter the keyword `count` then the number of debug outputs. The range is from 1 to 65534. The default is infinity.

Defaults None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

device–role

Specify the role of the device attached to the port.

Syntax

```
device-role {host | router}
```

To reset the device role, use the `no device-role {host | router}` command.

Parameters

host	Enter the keyword `host` to set the device-role as host.
router	Enter the keyword `router` to set the device-role as router.

Defaults None

Command Modes POLICY LIST CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Related Commands

- ipv6 nd raguard policy policy-name — define the RA guard policy name and enter the RA guard policy configuration mode.
- ipv6 nd ra-guard enable — configure the RA guard related commands.

hop–limit

Enable the verification of the advertised hop count limit. If this command is not configured, the verification process is bypassed.

Syntax `hop-limit {maximum | minimum limit}`

To reset the hop count limit, use the `no hop-limit {maximum | minimum limit}` command.

Parameters

maximum *limit*	Enter the keyword `maximum` then the hop limit value. The range is from 0 to 254.
minimum *limit*	Enter the keyword `minimum` then the hop limit value. The range is from 0 to 254.

Defaults None

Command Modes POLICY LIST CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the RA guard policy name and enter the RA guard policy configuration mode.

ipv6 nd ra–guard attach–policy

Apply the IPv6 RA guard to a specific interface.

Syntax `ipv6 nd ra-guard attach–policy policy-name [vlan [vlan 1, vlan 2, vlan 3.....]]`

Parameters

policy *policy-name*	Enter the keyword `policy` then the policy name. The policy-name allows a maximum of **140** characters.
vlan *[vlan 1, vlan 2, vlan 3.....]*	Enter the keyword `vlan` then the VLAN range. The VLAN range is from 1 to 4094.

Defaults None

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Related Commands

- show ipv6 nd ra-guard policy — display the configuration applied on all the RA guard policies or a specific RA guard policy.

ipv6 nd ra–guard enable

Allow you to configure the RA guard related commands.

Syntax `ipv6 nd ra-guard enable`

To disable the RA guard, use the `no ipv6 nd ra-guard enable` command.

Defaults Disabled

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.10(0.0)	Introduced on the S6100-ON.
9.9(0.0)	Introduced on the Z9500.

Version	Description
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

ipv6 nd ra–guard policy

Define the RA guard policy name and enter the RA guard policy list configuration mode.

Syntax `ipv6 nd ra-guard policy policy-name`

Parameters

policy *policy-name*	Enter the keyword `policy` then the policy-name. The policy name allows a maximum of **140** characters.

Defaults None

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.

managed-config-flag

Set the managed address configuration flag.

Syntax `managed-config-flag {on | off}`

To clear the flag, use the `no managed-config-flag {on | off}` command.

Parameters

on	Enter the keyword `on` to set the managed-config-flag value as ON.
off	Enter the keyword `off` to set the managed-config flag value as OFF.

Defaults None

Command Modes POLICY LIST CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

match ra

Enable verifying either of the configured source IPv6 address or prefix address or the source MAC address in the inspected messages. If this command is not configured, the verification process is bypassed.

Syntax

`match ra {ipv6-access-list` *`name`* `| ipv6-prefix-list` *`name`* `| mac-access-list` *`name`*`}`

To reset the access list, use the `no match ra{ipv6-access-list | ipv6-prefix-list | mac-access-list}` command.

Parameters

ipv6–access-list *name*	Enter the keywords `ipv6-access-list` then the access-list name. The access-list name allows a maximum of **140** characters.
ipv6–prefix-list *name*	Enter the keywords `ipv6-prefix-list` then the prefix-list name. The prefix-list name allows a maximum of **140** characters.
ipv6–mac-access-list *name*	Enter the keywords `ipv6-mac-access-list` then the mac-access-list name. The mac-access-list name allows a maximum of **140** characters.

Defaults

None

Command Modes

POLICY LIST CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000–ON.

Version	Description
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the RA guard policy name and enter the RA guard policy configuration mode.

mtu

Enable the verification of the configured maximum transmission unit (MTU) value in the received RA packets.

Syntax `mtu value`

To reset the MTU value, use the `no mtu value` command.

Parameters

value	Enter the maximum transmission unit value in bytes. The range is from 1,280 to 11,982 bytes.

Defaults 0

Command Modes POLICY LIST CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000–ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the RA guard policy name and enter the RA guard policy configuration mode.

other–config–flag

Enable the verification of the advertised other configuration parameter. If this command is not configured, the verification process is bypassed.

Syntax `other-config-flag {on | off}`

To reset the other configuration parameter, use the `no other-config-flag {on | off}` command.

Parameters

on	Enter the keyword `on` to set the other-config-flag value as ON.
off	Enter the keyword `off` to set the other-config flag value as OFF.

Defaults None

Command Modes POLICY LIST CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000–ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

reachable–time

Enable the verification of the configured reachability time in the received RA packets.

Syntax `reachable–time` *value*

To reset the advertised reachability time, use the `no reachable-time`*value* command.

Parameters

value	Enter the advertised reachability time in milliseconds. The range is from 0 to 3,600,000 milliseconds.

Defaults None

Command Modes POLICY LIST CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.

Version	Description
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the RA guard policy name and enter the RA guard policy configuration mode.

retrans-time

Enable the verification of the configured retransmission timer value in the received RA packets.

Syntax `retrans–timer value`

To reset the advertised retransmission interval, use the `no retrans-timervalue` command.

Parameters

value	Enter the advertised retransmission time interval in milliseconds. The range is from 100 to 4,294,967,295 milliseconds.

Defaults None

Command Modes POLICY LIST CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Related Commands ipv6 nd raguard policy policy-name — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

ipv6 nd ra-guard enable — configure the RA guard related commands.

router–lifetime

Set the router lifetime.

Syntax `router–lifetime value`

Parameters

value	Enter the router lifetime in seconds. The range is from 0 to 9,000 seconds.

Defaults None

Command Modes POLICY LIST CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

router–preference maximum

Enable the verification of the advertised default router preference (DRP) value. The preference value is lower than or equal to the specified limit. If this command is not configured, the verification process is bypassed.

Syntax

```
router-preference maximum {high | low | medium}
```

To reset the default router preference value, use the `no router-preference maximum {high | low | medium}` command.

Parameters

high	Enter the keyword `high` to set the DRP value as high.
low	Enter the keyword `low` to set the DRP value as low.
medium	Enter the keyword `medium` to set the DRP value as medium.

Defaults

None

Command Modes

POLICY LIST CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9000 switches.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.

- ipv6 nd raguard policy policy-name — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

show config

Display the RA guard policy mode configurations.

Syntax `show config`

Command Modes POLICY LIST CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Example

```
Dell(conf)# ipv6 nd ra-guard policy test
Dell(conf-ra_guard_policy_list)#show config
!
ipv6 nd ra-guard policy test
 device-role router
 hop-limit maximum 251
 mtu 1350
 other-config-flag on
 reachable-time 540
 retrans-timer 101
 router-preference maximum medium
 trusted-port
Dell(conf-ra_guard_policy_list)#
```

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd ra-guard policy — define the RA guard policy name and enter the RA guard policy list configuration mode.
- device-role — specify the role of the device attached to the port.
- hop-limit — enable the verification of the advertised hop count limit.
- mtu — set the maximum transmission unit (MTU) value.
- other-config-flag — enable the verification of the advertised other configuration parameter.
- reachable-time — set the advertised reachability time.
- retrans-timer — set the advertised retransmission time.
- router-preference maximum — enable the verification of the advertised default router preference (DRP) value.
- trusted-port — apply the policy to trusted ports.

show ipv6 nd ra–guard policy

Display the configurations applied on all the RA guard policies or a specific RA guard policy.

Syntax `show ipv6 nd ra-guard policy policy-name`

Parameter

policy *policy-name*	Enter the keyword `policy` then the policy name. The policy name allows a maximum of **140** characters.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, Introduced on the S6000–ON, and Z9000 switches.

Example

```
Dell# show ipv6 nd ra-guard policy test

ipv6 nd ra-guard policy test
  device-role router
  hop-limit maximum    1
  match  ra  ipv6-access-list  access
  other-config-flag on
  router-preference maximum medium
  trusted-port
  Interfaces :
  Te 6/1
Dell#
```

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd ra-guard policy — define the RA guard policy name and enter the RA guard policy list configuration mode.
- device-role — specify the role of the device attached to the port.
- hop-limit — enable the verification of the advertised hop count limit.
- mtu — set the maximum transmission unit (MTU) value.
- other-config-flag — enable the verification of the advertised other configuration parameter.
- reachable-time — set the advertised reachability time.
- retrans-timer — set the advertised retransmission time.
- router-preference maximum — enable the verification of the advertised default router preference (DRP) value.
- trusted-port — apply the policy to trusted ports.

- ipv6 nd raguard attach-policy — apply the IPv6 RA guard to a specific interface.

trusted–port

Allow bypassing the configured RA guard validation and forwards the RA packets received on the interface, which has the trusted port policy attached.

Syntax

`trusted-port`

To reset the policy applied to the trusted port, use the `no trusted-port` command.

Defaults

None

Command Modes

POLICY LIST CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the C9010.
9.9(0.0)	Introduced on the Z9500.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9000 switches.

Usage Information

Use this command to disable all the RA guard policies.

Related Commands

- ipv6 nd ra-guard enable — configure the RA guard related commands.
- ipv6 nd raguard policy policy-name — define the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

38

Object Tracking

Object Tracking supports IPv4 and IPv6 protocols.

Object tracking allows you to define objects of interest, monitor their state, and report to a client when a change in an object's state occurs. The following tracked objects are supported:

- Link status of Layer 2 interfaces
- Routing status of Layer 3 interfaces (IPv4 and IPv6)
- Reachability of IPv4 and IPv6 routes
- Metric thresholds of IPv4 and IPv6 routes

You can configure client applications, such virtual router redundancy protocol (VRRP), to receive a notification when the state of a tracked object changes.

This chapter contains the following sections:

- IPv4 Object Tracking Commands
- IPv6 Object Tracking Commands

Topics:

- IPv4 Object Tracking Commands
- IPv6 Object Tracking Commands

IPv4 Object Tracking Commands

The following section describes the IPv4 object tracking commands.

debug track

Enable debugging for tracked objects.

C9000 Series

Syntax `debug track [all | notifications | object-id]`

Parameters

all	Enables debugging on the state and notifications of all tracked objects.
notifications	Enables debugging on the notifications of all tracked objects.
object-id	Enables debugging on the state and notifications of the specified tracked object. The range is from 1 to 500.

Defaults Enable debugging on the state and notifications of all tracked objects (`debug track all`).

Command Modes

- EXEC

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Example

```
Dell#debug track all

04:35:04: %RPM0-P:RP2 %OTM-5-STATE: track 6 - Interface TenGigabitEthernet
1/2/1
line-protocol DOWN

04:35:04: %RPM0-P:RP2 %OTM-5-NOTIF: VRRP notification: resource ID 6 DOWN
```

delay

Configure the time delay used before communicating a change in the status of a tracked object to clients.

C9000 Series

Syntax

`delay {[up seconds] [down seconds]}`

To return to the default setting, use the `no delay` command.

Parameters

seconds	Enter the number of seconds the object tracker waits before sending a notification about the change in the UP and/or DOWN state of a tracked object to clients. The range is 0 to 180. The default is **0 seconds**.

Defaults

0 seconds

Command Modes

OBJECT TRACKING (*conf_track_object-id*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information

To set the time delay before a change in the state of a tracked object is communicated to clients configure an UP and/or DOWN timer for each tracked object. The configured time delay starts when the state changes from UP to DOWN or vice-versa.

If the state of an object changes back to its former UP/DOWN state before the timer expires, the timer is cancelled and the client is not notified. For example, if the DOWN timer is running when an interface goes down and comes back up, the DOWN timer is cancelled and the client is not notified of the event.

If the timer expires and an object's state has changed, a notification is sent to the client. If you do not configure a delay timer, a notification is sent immediately after a change in the state of a tracked object is detected. The time delay in communicating a state change is specified in seconds.

Related Commands

- track interface ip routing – configures object tracking on the routing status of an IPv4 Layer 3 interface.
- track interface line-protocol – configures object tracking on the line-protocol state of a Layer 2 interface.
- track ip route metric threshold – configures object tracking on the threshold of an IPv4 route metric.
- track ip route reachability – configures object tracking on the reachability of an IPv4 route.

description

Enter a description of a tracked object.

C9000 Series

Syntax

`description {text}`

To remove the description, use the `no description {text}` command.

Parameters

text	Enter a description to identify a tracked object (80 characters maximum).

Defaults

none

Command Modes

OBJECT TRACKING (*conf_track_object-id*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.

Version	Description
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Related Commands

- track interface ip routing – configures object tracking on the routing status of an IPv4 Layer 3 interface.
- track interface line-protocol – configures object tracking on the line-protocol state of a Layer 2 interface.
- track ip route metric threshold – configures object tracking on the threshold of an IPv4 route metric.
- track ip route reachability – configures object tracking on the reachability of an IPv4 route.

show running-config track

Display the current configuration of tracked objects.

C9000 Series

Syntax `show running-config track [object-id]`

Parameters

object-id	(OPTIONAL) Display information on the specified tracked object. The range is 1 to 500.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Example

```
Dell#show running-config track

track 1 ip route 23.0.0.0/8 reachability

track 2 ipv6 route 2040::/64 metric threshold
delay down 3
delay up 5
threshold metric up 200

track 3 ipv6 route 2050::/64 reachability

track 4 interface TenGigabitEthernet 1/2/1 ip routing

track 5 ip route 192.168.0.0/24 reachability vrf red

track resolution ip route isis 20
track resolution ip route ospf 10
```

Example (Object-id)

```
Dell#show running-config track 300

track 300 ip route 10.0.0.0/8 metric threshold
```

```
delay down 3
delay up 5
threshold metric up 100
```

Related Commands

- show track – displays information about tracked objects, including configuration, current state, and clients which track the object.
- track interface ip routing – configures object tracking on the routing status of an IPv4 Layer 3 interface.
- track interface line-protocol – configures object tracking on the line-protocol state of a Layer 2 interface.
- track ip route metric threshold – configures object tracking on the threshold of an IPv4 route metric.
- track ip route reachability – configures object tracking on the reachability of an IPv4 route.

show track

Display information about tracked objects, including configuration, current tracked state (UP or DOWN), and the clients which are tracking an object.

C9000 Series

Syntax

```
show track [object-id [brief] | interface [brief] [vrf vrf-name] | ip route
[brief] [vrf vrf-name] | resolution | vrf vrf-name [brief] | brief]
```

Parameters

object-id	(OPTIONAL) Display information on the specified tracked object. The range is 1 to 500.
interface	(OPTIONAL) Display information on all tracked interfaces (Layer 2 and IPv4 Layer 3).
ip route	(OPTIONAL) Display information on all tracked IPv4 routes.
resolution	(OPTIONAL) Display information on the configured resolution values used to scale protocol-specific route metrics. The range is 0 to 255.
brief	(OPTIONAL) Display a single line summary of the tracking information for a specified object, object type, or all tracked objects.
vrf *vrf-name*	(OPTIONAL) E-Series only: Display information on only the tracked objects that are members of the specified VRF instance. The maximum is 32 characters. If you do not enter a VRF name, information on the tracked objects from all VRFs displays.

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information The following describes the `show track` command shown in the Example below.

Output	Description
Track ***object-id***	Displays the number of the tracked object.

Output	Description
Interface *type slot/port*, IP route *ip-address*, IPv6 route *ipv6-address*	Displays the interface type and slot/port number or address of the IPv4/IPv6 route that is being tracked.
object is Up/Down	Up/Down state of tracked object; for example, IPv4 interface, reachability or metric threshold of an IP route.
number changes, last change *time*	Number of times that the state of the tracked object has changed and the time since the last change in *hours:minutes:seconds*.
First hop interface	Displays the type and slot/port number of the first-hop interface of the tracked route.
Tracked by	Client that is tracking an object's state; for example, VRRP.

The following describes the `show track brief` command shown in the Example below.

Output	Description
ResID	Number of the tracked object.
Resource	Type of tracked object.
Parameter	Detailed description of the tracked object.
State	Up or Down state of the tracked object.
Last Change	Time since the last change in the state of the tracked object.

Example

```
Dell#show track

Track 1
  IP route 23.0.0.0/8 reachability
  Reachability is Down (route not in route table)
    2 changes, last change 00:16:08
  Tracked by:

Track 2
  IPv6 route 2040::/64 metric threshold
  Metric threshold is Up (STATIC/0/0)
    5 changes, last change 00:02:16
  Metric threshold down 255 up 254
  First-hop interface is TenGigabitEthernet 1/2/1
  Tracked by:
    VRRP TenGigabitEthernet 2/3/4 IPv6 VRID 1

Track 3
  IPv6 route 2050::/64 reachability
  Reachability is Up (STATIC)
    5 changes, last change 00:02:16
  First-hop interface is TenGigabitEthernet 1/2/1
  Tracked by:
    VRRP TenGigabitEthernet 2/3/4 IPv6 VRID 1
```

Example (Brief)

```
Dell>show track brief
ResId Resource               Parameter   State LastChange
1     IP route reachability   10.16.0.0/16 Up   00:01:08
2     Interface line-protocol Ethernet0/2  Down 00:05:00
3     Interface ip routing    VLAN100      Up   01:10:05
```

Related Commands

- show running-config track – displays configuration information about tracked objects.
- track interface ip routing – configures object tracking on the routing status of an IPv4 Layer 3 interface.

- track interface line-protocol – configures object tracking on the line-protocol state of a Layer 2 interface.
- track ip route metric threshold – configures object tracking on the threshold of an IPv4 route metric.
- track ip route reachability – configures object tracking on the reachability of an IPv4 route.
-

threshold metric

Configure the metric threshold used to determine the UP and/or DOWN state of a tracked IPv4 or IPv6 route.

C9000 Series

Syntax

`threshold metric {up` *`number`* `| down` *`number`*`}`

To return to the default setting, use the `no threshold metric {up` *`number`* `| down` *`number`*`}` command.

Parameters

up *number*	Enter a number for the UP threshold to be applied to the scaled metric of an IPv4 or IPv6 route. The default UP threshold is **254**. The routing state is UP if the scaled route metric is less than or equal to the UP threshold.
down *number*	Enter a number for the DOWN threshold to be applied to the scaled metric of an IPv4 or IPv6 route. The default DOWN threshold is **255**. The routing state is DOWN if the scaled route metric is greater than or equal to the DOWN threshold.

Defaults

none

Command Modes

OBJECT TRACKING (conf_track_*object-id*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information

Determine the UP/DOWN state of a tracked route by the threshold for the current value of the route metric in the routing table. To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible. The scaled metric value communicated to a client always considers a lower value to have priority over a higher value.

The resulting scaled value is compared against the configured threshold values to determine the state of a tracked route as follows:

- If the scaled metric for a route entry is less than or equal to the UP threshold, the state of a route is UP.

- If the scaled metric for a route is greater than or equal to the DOWN threshold or the route is not entered in the routing table, the state of a route is DOWN.

Configure the UP and DOWN thresholds for each tracked route with the `threshold metric` command. The default UP threshold is **254**; the default DOWN threshold is **255**. The notification of a change in the state of a tracked object is sent when a metric value crosses a configured threshold.

The tracking process uses a protocol-specific resolution value to convert the actual metric in the routing table to a scaled metric in the range 0 to 255. You can configure the resolution value used to scale route metrics for supported protocols with the `track resolution ip route` and `track resolution ipv6 route` commands.

Related Commands

- track ip route metric threshold – configures object tracking on the threshold of an IPv4 route metric.
- track resolution ip route – configures the protocol-specific resolution value used to scale an IPv4 route metric.

track interface ip routing

Configure object tracking on the routing status of an IPv4 Layer 3 interface.

C9000 Series

Syntax

`track` *`object-id`* `interface` *`interface`* `ip routing`

To return to the default setting, use the `no track` *`object-id`* command.

Parameters

object-id	Enter the ID number of the tracked object. The range is from 1 to 500.
interface	Enter one of the following values: • For a 1-Gigabit Ethernet interface, enter `gigabitethernet` and the slot-number/ port-number. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a port channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter `tengigabitethernet` and the slot-number/ port-number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information Use this command to create an object that tracks the routing state of an IPv4 Layer 3 interface:

- The status of the IPv4 interface is UP only if the Layer 3 status of the interface is UP and the interface has a valid IP address.
- The Layer 3 status of an IPv4 interface goes DOWN when its Layer 3 status goes down (for a Layer 3 VLAN, all VLAN ports must be down) or the IP address is removed from the routing table.

Related Commands

- show track – displays information about tracked objects, including configuration, current state, and clients which track the object.
- track interface line-protocol – configures object tracking on the line-protocol state of a Layer 2 interface.

track interface line-protocol

Configure object tracking on the line-protocol state of a Layer 2 interface.

C9000 Series

Syntax `track object-id interface interface line-protocol`

To return to the default setting, use the `no track object-id` command.

Parameters

object-id	Enter the ID number of the tracked object. The range is 1 to 500.
interface	Enter one of the following values: • For a 1-Gigabit Ethernet interface, enter `gigabitethernet` and the slot-number/ port-number. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a port channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter `tengigabitethernet` and the slot-number/ port-number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information

Use this command to create an object that tracks the line-protocol state of a Layer 2 interface by monitoring its operational status (UP or DOWN).

When the link-level status goes down, the tracked object status is considered to be DOWN; if the link-level status is up, the tracked object status is considered to be UP.

Related Commands

- show track – displays information about tracked objects, including configuration, current state, and clients which track the object.
- track interface ip routing – configures object tracking on the routing status of an IPv4 Layer 3 interface.

track ip route metric threshold

Configure object tracking on the threshold of an IPv4 route metric.

C9000 Series

Syntax

`track` *`object-id`* `ip route` *`ip-address/prefix-len`* `metric threshold`

To return to the default setting, use the `no track object-id` command.

Parameters

object-id	Enter the ID number of the tracked object. The range is 1 to 500.
ip-address/ prefix-len	Enter an IPv4 address in dotted decimal format. The valid IPv4 prefix lengths are from /0 to /32.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.

Version	Description
8.4.1.0	Introduced.

Usage Information

Use this command to create an object that tracks the UP and/or DOWN threshold of an IPv4 route metric. In order for a route's metric to be tracked, the route must appear as an entry in the routing table.

A tracked IPv4 route is considered to match an entry in the routing table only if the exact IPv4 address and prefix length match a table entry. For example, when configured as a tracked route, 10.0.0.0/24 does not match the routing table entry 10.0.0.0/8. If no route-table entry has the exact IPv4 address and prefix length, the status of the tracked route is considered to be DOWN.

When you configure the threshold of an IPv4 route metric as a tracked object, the UP/DOWN state of the tracked route is also determined by the current metric for the route in the routing table.

To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible. The scaled metric value communicated to a client always considers a lower value to have priority over a higher value. The resulting scaled value is compared against the configured threshold values to determine the state of a tracked route as follows:

- If the scaled metric for a route entry is less than or equal to the UP threshold, the state of a route is UP.
- If the scaled metric for a route is greater than or equal to the DOWN threshold or the route is not entered in the routing table, the state of a route is DOWN.

You configure the UP and DOWN thresholds for each tracked route by using the `threshold metric` command. The default UP threshold is **254**; the default DOWN threshold is **255**. The notification of a change in the state of a tracked object is sent when a metric value crosses a configured threshold.

Related Commands

- show track – displays information about tracked objects, including configuration, current state, and clients which track the object.
- threshold metric – configures the metric threshold used to determine the UP and/or DOWN state of a tracked route.
- track resolution ip route – configures the protocol-specific resolution value used to scale an IPv4 route metric.

track ip route reachability

Configure object tracking on the reachability of an IPv4 route.

C9000 Series

Syntax

`track` *`object-id`* `ip route` *`ip-address/prefix-len`* `reachability`

To return to the default setting, use the `no track` *`object-id`* command.

Parameters

object-id	Enter the ID number of the tracked object. The range is from 1 to 500.
ip-address/ prefix-len	Enter an IPv4 address in dotted decimal format. The valid IPv4 prefix lengths are from /0 to /32.

Defaults none

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information

Use this command to create an object that tracks the reachability of an IPv4 route. In order for a route's reachability to be tracked, the route must appear as an entry in the routing table.

A tracked IPv4 route is considered to match an entry in the routing table only if the exact IPv4 address and prefix length match a table entry. For example, when configured as a tracked route, 10.0.0.0/24 does not match the routing table entry 10.0.0.0/8. If no route-table entry has the exact IPv4 address and prefix length, the status of the tracked route is considered to be DOWN.

When you configure IPv4 route reachability as a tracked object, the UP/DOWN state of the tracked route is also determined by the entry of the next-hop address in the address resolution protocol (ARP) cache. A tracked route is considered to be reachable if there is an ARP cache entry for the route's next-hop address.

If the next-hop address in the ARP cache ages out for a route tracked for its reachability, an attempt is made to regenerate the ARP cache entry if the next-hop address appears before considering the route DOWN.

Related Commands

- show track – displays information about tracked objects, including configuration, current state, and clients which track the object.
- track ip route metric threshold – configures object tracking on the threshold of an IPv4 route metric.

track reachability refresh

Change the refresh interval for tracking the reachability of the next-hop. If the next-hop address in the ARP cache ages out for a route tracked for its reachability, an attempt is made to check if the next-hop address is reachable after a certain refresh interval before considering the route DOWN.

Syntax

```
track reachability refresh interval
```

Parameters

interval	Enter the refresh interval, in seconds, for object tracking reachability. The range is from 0 to 60 seconds. The default is 60.

Defaults

Enabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information To disable the attempt to track the reachability of next-hop after the configured refresh interval, set the refresh interval as 0.

Related Commands

- show track – display information about tracked objects, including configuration, current state, and clients which track the object.
- track ip route metric threshold – configure object tracking on the threshold of an IPv4 route metric.

track resolution ip route

Configure the protocol-specific resolution value used to scale an IPv4 route metric.

C9000 Series

Syntax `track resolution ip route {isis` *`resolution-value`* `| ospf` *`resolution-value`*`}`

To return to the default setting, use the `no track` *`object-id`* command.

Parameters

object-id	Enter the ID number of the tracked object. The range is from 1 to 500.
isis ***resolution-value***	Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.
ospf ***resolution-value***	Enter the resolution used to convert the metric in the routing table for OSPF routes to a scaled metric.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information

Use this command to configure the protocol-specific resolution value that converts the actual metric of an IPv4 route in the routing table to a scaled metric in the range from 0 to 255.

The UP/DOWN state of a tracked IPv4 route is determined by a user-configurable threshold (the `threshold metric` command) for the route's metric in the routing table. To provide a common tracking interface for different clients, route metrics are scaled in the range of 0-255, where 0 is connected and 255 is inaccessible.

The protocol-specific resolution value calculates the scaled metric by dividing a route's cost by the resolution value set for the route protocol:

- For ISIS, you can set the resolution in the range of 1-1000, where the default is **10**.
- For OSPF, you can set the resolution in the range of 1-1592, where the default is **1**.
- You cannot configure the resolution value used to map static routes. By default, Dell Networking OS assigns a metric of **0** to static routes.
- You cannot configure the resolution value used to map RIP routes. The RIP hop-count is automatically multiplied by 16 to scale it. For example, a RIP metric of 16 (unreachable) scales to 256, which considers the route to be DOWN.

Related Commands

- threshold metric – configures the metric threshold used to determine the UP and/or DOWN state of a tracked route.
- track ip route metric threshold – configures object tracking on the threshold of an IPv4 route metric.

IPv6 Object Tracking Commands

The following section describes the IPv6 object tracking commands.

The following object tracking commands apply to IPv4 and IPv6:

- debug track
- delay
- description
- show running-config track
- threshold metric
- track interface line-protocol

show track ipv6 route

Display information about all tracked IPv6 routes, including configuration, current tracked state (UP or DOWN), and the clients which are tracking an object.

C9000 Series

Syntax

```
show track ipv6 route [brief]
```

Parameters

brief	(OPTIONAL) Display a single line summary of information for tracked IPv6 routes.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Command

The following table describes the `show track ipv6 route` command shown in the following example.

Output	Description
Track *object-id*	Displays the number of the tracked object.
Interface *type slot/port*, IP route *ip-address*, IPv6 route *ipv6-address*	Displays the interface type and slot/port number or address of the IPv4/IPv6 route that is being tracked.
object is Up/Down	Up/Down state of tracked object; for example, IPv4 interface, reachability, or metric threshold of an IP route.
number changes, last change *time*	Number of times that the state of the tracked object has changed and the time since the last change in *hours:minutes:seconds*.
First hop interface	Displays the type and slot/port number of the first-hop interface of the tracked route.
Tracked by	Client that is tracking an object's state; for example, VRRP.

The following table describes the `show track ipv6 route brief` command shown in the example.

Ouput	Description
ResID	Number of the tracked object.
Resource	Type of tracked object.
Parameter	Detailed description of the tracked object.
State	Up or Down state of the tracked object.
Last Change	Time since the last change in the state of the tracked object.

Example

```
Dell#show track ipv6 route

Track 2
  IPv6 route 2040::/64 metric threshold
  Metric threshold is Up (STATIC/0/0)
    5 changes, last change 00:02:30
  Metric threshold down 255 up 254
  First-hop interface is TenGigabitEthernet 1/2/1
  Tracked by:
    VRRP TenGigabitEthernet 2/4/1 IPv6 VRID 1

Track 3
  IPv6 route 2050::/64 reachability
  Reachability is Up (STATIC)
    5 changes, last change 00:02:30
  First-hop interface is TenGigabitEthernet 1/2/1
  Tracked by:
    VRRP TenGigabitEthernet 2/4/1 IPv6 VRID
```

Example (Brief)

```
Dell#show track ipv6 route brief

ResId Resource                  Parameter State LastChange
2     IPv6 route metric threshold 2040::/64 Up 00:02:36
3     IPv6 route reachability     2050::/64 Up 00:02:36
```

Related Commands

- show running-config track – displays configuration information about tracked objects.
- show track – displays information about tracked objects, including configuration, current state, and clients which track the object.
- track interface ipv6 routing – configures object tracking on the routing status of an IPv6 Layer 3 interface.
- track ipv6 route metric threshold – configures object tracking on the threshold of an IPv6 route metric.
- track ipv6 route reachability – configures object tracking on the reachability of an IPv6 route.

track interface ipv6 routing

Configure object tracking on the routing status of an IPv6 Layer 3 interface.

C9000 Series

Syntax

`track object-id interface interface ipv6 routing`

To return to the default setting, use the `no track object-id` command.

Parameters

object-id	Enter the ID number of the tracked object. The range is from 1 to 500.

interface Enter one of the following values:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information Use this command to create an object that tracks the routing state of an IPv6 Layer 3 interface:

- The status of the IPv6 interface is UP only if the Layer 2 status of the interface is UP and the interface has a valid IP address.
- The Layer 3 status of an IPv6 interface goes DOWN when its Layer 2 status goes down (for a Layer 3 VLAN, all VLAN ports must be down) or the IP address is removed from the routing table.

Related Commands

- show track ipv6 route – displays information about tracked IPv6 routes, including configuration, current state, and clients which track the route.
- track interface ip routing – configures object tracking on the routing status of an IPv4 Layer 3 interface.

track ipv6 route metric threshold

Configure object tracking on the threshold of an IPv4 route metric.

C9000 Series

Syntax `track object-id ipv6 route ipv6-address/prefix-len metric threshold`

To return to the default setting, use the `no track object-id` command.

Parameters

object-id	Enter the ID number of the tracked object. The range is from 1 to 500.
ipv6-address/ prefix-len	Enter an IPv6 address in X:X:X:X::X format. The valid IPv6 prefix lengths are from /0 to /128.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information Use this command to create an object that tracks the UP and/or DOWN threshold of an IPv6 route metric. In order for a route's metric to be tracked, the route must appear as an entry in the routing table.

A tracked IPv6 route is considered to match an entry in the routing table only if the exact IPv6 address and prefix length match a table entry. For example, when configured as a tracked route, 3333:100:200:300:400::/80 does not match routing table entry 3333:100:200:300::/64. If no route-table entry has the exact IPv6 address and prefix length, the status of the tracked route is considered to be DOWN.

When you configure the threshold of an IPv6 route metric as a tracked object, the UP/DOWN state of the tracked route is also determined by the current metric for the route in the routing table.

To provide a common tracking interface for different clients, route metrics are scaled in the range 0 to 255, where 0 is connected and 255 is inaccessible. The scaled metric value communicated to a client always considers a lower value to have priority over a higher value. To determine the state of a tracked route, the resulting scaled value is compared against the configured threshold values as follows:

- If the scaled metric for a route entry is less than or equal to the UP threshold, the state of a route is UP.
- If the scaled metric for a route is greater than or equal to the DOWN threshold or the route is not entered in the routing table, the state of a route is DOWN.

Configure the UP and DOWN thresholds for each tracked IPv6 route using the `threshold metric` command. The default UP threshold is **254**; the default DOWN threshold is **255**. The notification of a change in the state of a tracked object is sent when a metric value crosses a configured threshold.

Related Commands

- show track ipv6 route – displays information about tracked IPv6 routes, including configuration, current state, and clients which track the route.
- threshold metric – configures the metric threshold used to determine the UP and/or DOWN state of a tracked route.

- track resolution ipv6 route – configures the protocol-specific resolution value used to scale an IPv6 route metric.

track ipv6 route reachability

Configure object tracking on the reachability of an IPv6 route.

Syntax

`track object-id ipv6 route ip-address/prefix-len reachability`

To return to the default setting, use the `no track object-id` command.

Parameters

object-id	Enter the ID number of the tracked object. The range is from 1 to 500.
ipv6-address/ prefix-len	Enter an IPv6 address in X:X:X:X::X format. The valid IPv6 prefix lengths are from /0 to /128.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information

Use this command to create an object that tracks the reachability of an IPv6 route. In order for a route's reachability to be tracked, the route must appear as an entry in the routing table.

A tracked route is considered to match an entry in the routing table only if the exact IPv6 address and prefix length match a table entry. For example, when configured as a tracked route, 3333:100:200:300:400::/80 does not match routing table entry 3333:100:200:300::/64. If no route-table entry has the exact IPv6 address and prefix length, the tracked route is considered to be DOWN.

When you configure IPv6 route reachability as a tracked object, the UP/DOWN state of the tracked route is also determined by the entry of the next-hop address in the ARP cache. A tracked route is considered to be reachable if there is an ARP cache entry for the route's next-hop address.

If the next-hop address in the ARP cache ages out for a route tracked for its reachability, an attempt is made to regenerate the ARP cache entry to if the next-hop address appears before considering the route DOWN.

Related Commands

- show track ipv6 route – displays information about tracked IPv6 routes, including configuration, current state, and clients which track the route.
- track ipv6 route reachability – configures object tracking on the reachability of an IPv4 route.

track reachability refresh

Change the refresh interval for tracking the reachability of the next-hop. If the next-hop address in the ARP cache ages out for a route tracked for its reachability, an attempt is made to check if the next-hop address is reachable after a certain refresh interval before considering the route DOWN.

Syntax

```
track reachability refresh interval
```

Parameters

interval	Enter the refresh interval, in seconds, for object tracking reachability. The range is from 0 to 60 seconds. The default is 60.

Defaults

Enabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information

To disable the attempt to track the reachability of next-hop after the configured refresh interval, set the refresh interval as 0.

Related Commands

- show track – display information about tracked objects, including configuration, current state, and clients which track the object.
- track ip route metric threshold – configure object tracking on the threshold of an IPv4 route metric.

track resolution ipv6 route

Configure the protocol-specific resolution value used to scale an IPv6 route metric.

C9000 Series

Syntax

```
track resolution ipv6 route {isis resolution-value | ospf resolution-value}
```

To return to the default setting, use the `no track object-id` command.

Parameters

object-id	Enter the ID number of the tracked object. The range is from 1 to 500.
isis *resolution-value*	Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.
ospf *resolution-value*	Enter the resolution used to convert the metric in the routing table for OSPF routes to a scaled metric.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced.

Usage Information

Use this command to configure the protocol-specific resolution value that converts the actual metric of an IPv6 route in the routing table to a scaled metric in the range of 0 to 255.

The UP/DOWN state of a tracked IPv6 route is determined by the user-configurable threshold (the `threshold metric` command) for a route's metric in the routing table. To provide a common tracking interface for different clients, route metrics are scaled in the range of 0 to 255, where 0 is connected and 255 is inaccessible.

The protocol-specific resolution value calculates the scaled metric by dividing a route's cost by the resolution value set for the route protocol:

- For ISIS, you can set the resolution in the range of 1 to 1000, where the default is 10.
- For OSPF, you can set the resolution in the range of 1 to 1592, where the default is 1.
- You cannot configure the resolution value used to map static routes. By default, Dell Networking OS assigns a metric of 0 to static routes.

- You cannot configure the resolution value used to map RIP routes. The RIP hop-count is automatically multiplied by 16 to scale it. For example, a RIP metric of 16 (unreachable) scales to 256, which considers the route to be DOWN.

Related Commands

- threshold metric – configures the metric threshold used to determine the UP and/or DOWN state of a tracked route.
- track ipv6 route metric threshold – configures object tracking on the threshold of an IPv6 route metric.

39

Open Shortest Path First (OSPFv2 and OSPFv3)

Open Shortest Path First (OSPF) is an Interior Gateway Protocol (IGP), which means that it distributes routing information between routers in a single Autonomous System (AS). OSPF is also a link-state protocol in which all routers contain forwarding tables derived from information about their links to their neighbors.

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) are the same for OSPFv2 and OSPFv3. OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis.

On Tunnel interfaces, OSPFv2 is supported on IPv6 tunnels only and OSPFv3 is supported on IPv4 tunnels only.

This chapter is divided into two sections. There is no overlap between the two sets of commands. You cannot use an OSPFv2 command in the IPv6 OSPFv3 mode.

- OSPFv2 Commands
- OSPFv3 Commands

OSPF on Tunnel Interfaces:

NOTE: The Dell Networking OS versions 9.4(0.0) and 9.7(0.0) introduce support for VRF on OSPFv2 and OSPFv3, respectively. The multi-process OSPF feature supported on Dell Networking OS version 7.8.1.0 is modified. In earlier versions, multiple OSPF processes were created without VRF (prior to 9.4 release). In Dell Networking OS version 9.4 and version 9.7 (for OSPFv3), multiple OSPF processes can be created on a router, but with only one OSPF process per VRF. However, there can be one OSFPv2 and one OSPFv3 on the same VRF.

Topics:

- OSPFv2 Commands
- OSPFv3 Commands

OSPFv2 Commands

The Dell Networking implementation of OSPFv2 is based on IETF RFC 2328. .

area default-cost

Set the metric for the summary default route the area border router (ABR) generates into the stub area. Use this command on the border routers at the edge of a stub area.

C9000 Series

Syntax `area area-id default-cost cost`

To return default values, use the `no area area-id default-cost` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
cost	Specifies the stub area's advertised external route metric. The range is from zero (0) to 65535.

Defaults *cost* = **1**; no areas are configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information In the Dell Networking operating software, `cost` is defined as reference bandwidth/bandwidth.

Related Commands area stub — creates a stub area.

area nssa

Specify an area as a not so stubby area (NSSA).

C9000 Series

Syntax `area area-id nssa [default-information-originate] [no-redistribution] [no-summary]`

To delete an NSSA, use the `no area area-id nssa` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
no-redistribution	(OPTIONAL) Specify that the `redistribute` command does not distribute routes into the NSSA. Only use this command in an NSSA area border router (ABR).

default-information-originate	(OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.
no-summary	(OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

area range

Summarize routes matching an address/mask at an area border router (ABR).

C9000 Series

Syntax `area area-id range ip-address mask [not-advertise]`

To disable route summarization, use the `no area area-id range ip-address mask` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
ip-address	Specify an IP address in dotted decimal format.
mask	Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).
not-advertise	(OPTIONAL) Enter the keywords `not-advertise` to set the status to DoNotAdvertise (that is, the Type 3 summary-LSA is suppressed and the component networks remain hidden from other areas.)

Defaults Not configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information Only the routes within an area are summarized, and that summary is advertised to other areas by the ABR. External routes are not summarized.

Related Commands area stub — creates a stub area.

router ospf — enters ROUTER OSPF mode to configure an OSPF instance.

area stub

Configure a stub area, which is an area not connected to other areas.

C9000 Series

Syntax `area area-id stub [no-summary]`

To delete a stub area, use the `no area area-id stub` command.

Parameters

area-id	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
no-summary	(OPTIONAL) Enter the keywords `no-summary` to prevent the ABR from sending summary Link State Advertisements (LSAs) into the stub area.

Defaults Disabled.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information To configure all routers and access servers within a stub, use this command.

Related Commands router ospf — enters ROUTER OSPF mode to configure an OSPF instance.

auto-cost

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

C9000 Series

Syntax `auto-cost [reference-bandwidth ref-bw]`

To return to the default bandwidth or to assign cost based on the interface type, use the `no auto-cost [reference-bandwidth]` command.

Parameters

ref-bw	(OPTIONAL) Specify a reference bandwidth in megabits per second. The range is from 1 to 4294967. The default is **100 megabits per second**.

Defaults **100 megabits per second**.

Command Modes ROUTER OSPFv3

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

clear ip ospf

Clear all OSPF routing tables.

C9000 Series

Syntax `clear ip ospf process-id [vrf {vrf name}]|[process]`

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
vrf name	Enter the VRF process identifier to tie the OSPF instance to the VRF. All network commands under this OSPF instance are then tied to the VRF instance.
process	(OPTIONAL) Enter the keyword `process` to reset the OSPF process.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4 (0.0)	Added support for VRF on all platforms (Except MXL and STOMP)
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

clear ip ospf statistics

Clear the packet statistics in interfaces and neighbors.

C9000 Series

Syntax `clear ip ospf process-id vrf vrf-name statistics [interface name {neighbor router-id}]`

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to clear all OSPF routing tables corresponding to that VRF
interface *name*	(OPTIONAL) Enter the keyword `interface` then one of the following interface keywords and slot/port or number information: • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Null interface, enter the keywords `null 0`. • For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
neighbor *router-id*	(OPTIONAL) Enter the keyword `neighbor` then the neighbor's router-id in dotted decimal format (A.B.C.D.).

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related Commands show ip ospf statistics — displays the OSPF statistics.

debug ip ospf

Display debug information on OSPF. Entering the `debug ip ospf` commands enables OSPF debugging for the first OSPF process.

C9000 Series

Syntax

`debug ip ospf` *`process-id`* `[vrf` *`vrf name`*`][bfd |event | packet | spf | database-timers]`

To cancel the debug command, use the `no debug ip ospf` command.

Parameters

process-id	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
vrf name	Enter the keyword `vrf` to view debugging information on OSPF corresponding to that VRF.
bfd	(OPTIONAL) Enter the keyword `bfd` to debug only OSPF BFD information.
event	(OPTIONAL) Enter the keyword `event` to debug only OSPF event information.
packet	(OPTIONAL) Enter the keyword `packet` to debug only OSPF packet information.
spf	(OPTIONAL) Enter the keyword `spf` to display the Shortest Path First information.
database-timers	(OPTIONAL) Enter the keywords `database-timers` to display the LSA throttling timer information.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Added the `database-timer rate-limit` option for the S4810.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information The following describes the `debug ip ospf` command shown in the Example below.

Field	Description
8:14	Displays the time stamp.
OSPF	Displays the OSPF process ID: instance ID.
v:	Displays the OSPF version. The system supports version 2 only.
t:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
l:	Displays the packet length.
rid:	Displays the OSPF router ID.
aid:	Displays the Autonomous System ID.
chk:	Displays the OSPF checksum.
aut:	States if OSPF authentication is configured. One of the following is listed: • 0 - no authentication configured • 1 - simple authentication configured using the `ip ospf authentication-key` command • 2 - MD5 authentication configured using the `ip ospf message-digest-key` command
auk:	If the `ip ospf authentication-key` command is configured, this field displays the key used.
keyid:	If the `ip ospf message-digest-key` command is configured, this field displays the MD5 key
to:	Displays the interface to which the packet is intended.
dst:	Displays the destination IP address.
netmask:	Displays the destination IP address mask.
pri:	Displays the OSPF priority
N, MC, E, T	Displays information available in the Options field of the HELLO packet: • N + (N-bit is set) • N - (N-bit is not set) • MC+ (bit used by MOSPF is set and router is able to forward IP multicast packets) • MC- (bit used by MOSPF is not set and router cannot forward IP multicast packets) • E + (router is able to accept AS External LSAs) • E - (router cannot accept AS External LSAs) • T + (router can support TOS) • T - (router cannot support TOS)
hi:	Displays the amount of time configured for the HELLO interval.

Field	Description
di:	Displays the amount of time configured for the DEAD interval.
dr:	Displays the IP address of the designated router.
bdr:	Displays the IP address of the Border Area Router.

Example

```
Dell#debug ip ospf 1 packet
OSPF process 90, packet debugging is on

Dell#
08:14:24 : OSPF(100:00):
Xmt. v:2 t:1(HELLO) l:44 rid:192.1.1.1
   aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:Te 1/3 dst:224.0.0.5
      netmask:255.255.255.0 pri:1 N-, MC-, E+, T-,
      hi:10 di:40 dr:90.1.1.1 bdr:0.0.0.0
```

default-information originate

To generate a default external route into an OSPF routing domain, configure the system.

C9000 Series

Syntax

`default-information originate [always] [metric` *`metric-value`*`] [metric-type` *`type-value`*`] [route-map` *`map-name`*`]`

To return to the default values, use the `no default-information originate` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to specify that default route information must always be advertised.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number to configure a metric value for the route. The range is from 1 to 16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then an OSPF link state type of 1 or 2 for default routes. The values are: • 1 = Type 1 external route • 2 = Type 2 external route
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map.

Defaults

Disabled.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related Commands redistribute — redistributes routes from other routing protocols into OSPF.

default-metric

Change the metrics of redistributed routes to a value useful to OSPF. Use this command with the `redistribute` command.

C9000 Series

Syntax `default-metric` *number*

To return to the default values, use the `no default-metric [number]` command.

Parameters

number	Enter a number as the metric. The range is from 1 to 16777214.

Defaults Disabled.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related Commands redistribute — redistributes routes from other routing protocols into OSPF.

description

Add a description about the selected OSPF configuration.

C9000 Series

Syntax `description description`

To remove the OSPF description, use the `no description` command.

Parameters

description	Enter a text string description to identify the OSPF configuration (80 characters maximum).

Defaults none

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

distance

Define an administrative distance for particular routes to a specific IP address.

C9000 Series

Syntax `distance weight [ip-address mask prefix-list-name]`

To delete the settings, use the `no distance weight [ip-address mask prefix-list-name]` command.

Parameters

weight	Specify an administrative distance. The range is from 1 to 255. The default is **110**.
ip-address	(OPTIONAL) Enter a router ID in the dotted decimal format. If you enter a router ID, include the mask for that router address.
mask	(OPTIONAL) Enter a mask in dotted decimal format or /n format.
prefix-list-name	(OPTIONAL) Enter the name of an IP standard prefix list, up to 140 characters.

Defaults **110**

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

distance ospf

Configure an OSPF distance metric for different types of routes.

C9000 Series

Syntax `distance ospf [external dist3] [inter-area dist2] [intra-area dist1]`

To delete these settings, use the `no distance ospf` command.

Parameters

external *dist3*	(OPTIONAL) Enter the keyword `external` then a number to specify a distance for external type 5 and 7 routes. The range is from 1 to 255. The default is **110**.
inter-area *dist2*	(OPTIONAL) Enter the keywords `inter-area` then a number to specify a distance metric for routes between areas. The range is from 1 to 255. The default is **110**.

intra-area *dist1* (OPTIONAL) Enter the keywords `intra-area` then a number to specify a distance metric for all routes within an area. The range is from 1 to 255. The default is **110**.

Defaults

- external *dist3* = **110**
- inter-area *dist2* = **110**
- intra-area *dist1* = **110**

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information To specify a distance for routes learned from other routing domains, use the `redistribute` command.

distribute-list in

Apply a filter to incoming routing updates from OSPF to the routing table.

C9000 Series

Syntax `distribute-list` *`prefix-list-name`* `in [`*`interface`*`]`

To delete a filter, use the `no distribute-list` *`prefix-list-name`* `in [`*`interface`*`]` command.

Parameters

prefix-list-name Enter the name of a configured prefix list.

interface (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

distribute-list out

To restrict certain routes destined for the local routing table after the SPF calculation, apply a filter.

C9000 Series

Syntax `distribute-list prefix-list-name out [bgp | connected | isis | rip | static]`

To remove a filter, use the `no distribute-list prefix-list-name out [bgp | connected | isis | rip | static]` command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
bgp	(OPTIONAL) Enter the keyword `bgp` to specify that BGP routes are distributed. **NOTE: BGP and ISIS routes are not available on the C-Series. BGP, ISIS, and RIP routes are not available on the S-Series.**
connected	(OPTIONAL) Enter the keyword `connected` to specify that connected routes are distributed.
isis	(OPTIONAL) Enter the keyword `isis` to specify that IS-IS routes are distributed. **NOTE: BGP and ISIS routes are not available on the C-Series. BGP, ISIS, and RIP routes are not available on the S-Series.**

rip	(OPTIONAL) Enter the keyword `rip` to specify that RIP routes are distributed. **NOTE: BGP and ISIS routes are not available on the C-Series. BGP, ISIS, and RIP routes are not available on the S-Series.**
static	(OPTIONAL) Enter the keyword `static` to specify that only manually configured routes are distributed.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information The `distribute-list out` command applies to routes autonomous system boundary routers (ASBRs) redistributes into OSPF. It can be applied to external type 2 and external type 1 routes, but not to intra-area and inter-area routes.

enable inverse-mask

By default, the system allows you to input the OSPF `network` command with a net-mask. This command provides a choice between inverse-mask or net-mask (the default).

C9000 Series

Syntax `enable inverse mask`

To return to the default net-mask, use the `no enable inverse mask` command.

Defaults **net-mask**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

fast-convergence

This command sets the minimum LSA origination and arrival times to zero (0), allowing more rapid route computation so that convergence takes less time.

C9000 Series

Syntax

`fast-convergence {number}`

To cancel fast-convergence, use the `no fast convergence` command.

Parameters

number	Enter the convergence level desired. The higher this parameter is set, the faster OSPF converge takes place. The range is from 1 to 4.

Defaults

none.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on all platforms.

Usage Information

The higher this parameter is set, the faster OSPF converge takes place.

NOTE: The faster the convergence, the more frequent the route calculations and updates. This behavior impacts CPU utilization and may impact adjacency stability in larger topologies.

Generally, convergence level 1 meets most convergence requirements. Higher convergence levels should only be selected following consultation with Dell Networking technical support.

graceful-restart grace-period

Specifies the time duration, in seconds, that the router's neighbors continue to advertise the router as fully adjacent regardless of the synchronization state during a graceful restart.

C9000 Series

Syntax

`graceful-restart grace-period` *seconds*

To disable the grace period, use the `no graceful-restart grace-period` command.

Parameters

seconds	Time duration, in seconds, that specifies the duration of the restart process before OSPF terminates the process. The range is from 40 to 1800 seconds.

Defaults

Not Configured

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series. Added support for Multi-Process OSPF.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

graceful-restart helper-reject

Specify the OSPF router to not act as a helper during graceful restart.

C9000 Series

Syntax

`graceful-restart helper-reject` *ip-address*

To return to default value, use the `no graceful-restart helper-reject` command.

Parameters

ip-address	Enter the OSPF router-id, in IP address format, of the restart router that *will not* act as a helper during graceful restart.

Defaults

Not configured.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	`Restart role` enabled on the S-Series (Both `Helper` and `Restart` roles now supported on S-Series). Added support for Multi-Process OSPF.
7.7.1.0	Added `Helper-Role` support on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

graceful-restart mode

Enable the graceful restart mode.

C9000 Series

Syntax

`graceful-restart mode [planned-only | unplanned-only]`

To disable graceful restart mode, use the `no graceful-restart mode` command.

Parameters

planned-only	(OPTIONAL) Enter the keywords `planned-only` to indicate graceful restart is supported in a planned restart condition only.
unplanned-only	(OPTIONAL) Enter the keywords `unplanned-only` to indicate graceful restart is supported in an unplanned restart condition only.

Defaults Support for both planned and unplanned failures.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

graceful-restart role

Specify the role for your OSPF router during graceful restart.

C9000 Series

Syntax `graceful-restart role [helper-only | restart-only]`

To disable graceful restart role, use the `no graceful-restart role` command.

Parameters

role helper-only	(OPTIONAL) Enter the keywords `helper-only` to specify the OSPF router is a helper only during graceful restart.
role restart-only	(OPTIONAL) Enter the keywords `restart-only` to specify the OSPF router is a restart only during graceful-restart.

Defaults By default, OSPF routers are both helper and restart routers during a graceful restart.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF. Added `Restart` and `Helper` roles support on the S-Series.
7.7.1.0	Added `Helper-Role` support on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

ip ospf auth-change-wait-time

OSPF provides a grace period while OSPF changes its interface authentication type. During the grace period, OSPF sends out packets with new and old authentication scheme until the grace period expires.

C9000 Series

Syntax

`ip ospf auth-change-wait-time` *seconds*

To return to the default, use the `no ip ospf auth-change-wait-time` command.

Parameters

seconds	Enter the seconds. The range is from 0 to 300.

Defaults

zero (0) seconds.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

ip ospf authentication-key

Enable authentication and set an authentication key on OSPF traffic on an interface.

C9000 Series

Syntax

```
ip ospf authentication-key [encryption-type] key
```

To delete an authentication key, use the `no ip ospf authentication-key` command.

Parameters

encryption-type	(OPTIONAL) Enter 7 to encrypt the key.
key	Enter an eight-character string. Strings longer than eight characters are truncated.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

All neighboring routers in the same network must use the same password to exchange OSPF information.

ip ospf cost

Change the cost associated with the OSPF traffic on an interface.

C9000 Series

Syntax

`ip ospf cost cost`

To return to default value, use the `no ip ospf cost` command.

Parameters

cost	Enter a number as the cost. The range is from 1 to 65535.

Defaults

The default cost is based on the reference bandwidth.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

If this command is not configured, cost is based on the `auto-cost` command.

When you configure OSPF over multiple vendors, to ensure that all routers use the same cost, use the `ip ospf cost` command. Otherwise, OSPF routes improperly.

Related Commands

auto-cost — controls how the OSPF interface cost is calculated.

ip ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the interval elapses, the neighboring routers declare the router dead.

C9000 Series

Syntax

```
ip ospf dead-interval seconds
```

To return to the default values, use the `no ip ospf dead-interval` command.

Parameters

seconds	Enter the number of seconds for the interval. The range is from 1 to 65535. The default is **40 seconds**.

Defaults **40 seconds**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information By default, the dead interval is four times the default hello-interval.

Related Commands ip ospf hello-interval — sets the time interval between the hello packets.

ip ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

C9000 Series

Syntax

```
ip ospf hello-interval seconds
```

To return to the default value, use the `no ip ospf hello-interval` command.

Parameters

seconds	Enter the number of seconds for the interval. The range is from 1 to 65535. The default is **10 seconds**.

Defaults **10 seconds**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information The time interval between the hello packets must be the same for routers in a network.

Related Commands ip ospf dead-interval — sets the time interval before a router is declared dead.

ip ospf message-digest-key

Enable OSPF MD5 authentication and send an OSPF message digest key on the interface.

C9000 Series

Syntax `ip ospf message-digest-key keyid md5 key`

To delete a key, use the `no ip ospf message-digest-key keyid` command.

Parameters

keyid	Enter a number as the key ID. The range is from 1 to 255.
key	Enter a continuous character string as the password.

Defaults No MD5 authentication is configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
9.1(0.0)	Included usage information on maximum number of digest keys per interface.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

You can configure a maximum of six digest keys on an interface. Of the available six digest keys, the switches select the MD5 key that is common. The remaining MD5 keys are unused.

To change to a different key on the interface, enable the new key while the old key is still enabled. The system sends two packets: the first packet authenticated with the old key and the second packet authenticated with the new key. This process ensures that the neighbors learn the new key and communication is not disrupted by keeping the old key enabled.

After the reply is received and the new key is authenticated, delete the old key. Dell recommends keeping only one key per interface.

NOTE: The MD5 secret is stored as plain text in the configuration file with service password encryption. Write down or otherwise record the key. You cannot learn the key once it is configured. Use caution when changing the key.

ip ospf mtu-ignore

Disable OSPF MTU mismatch detection upon receipt of database description (DBD) packets.

C9000 Series

Syntax

```
ip ospf mtu-ignore
```

To return to the default, use the `no ip ospf mtu-ignore` command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

ip ospf network

Set the network type for the interface.

C9000 Series

Syntax

```
ip ospf network {broadcast | point-to-point}
```

To return to the default, use the `no ip ospf network` command.

Parameters

broadcast	Enter the keyword `broadcast` to designate the interface as part of a broadcast network.
point-to-point	Enter the keywords `point-to-point` to designate the interface as part of a point-to-point network.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.1	Introduced on the E-Series.

ip ospf priority

To determine the designated router for the OSPF network, set the priority of the interface.

C9000 Series

Syntax

`ip ospf priority` *number*

To return to the default setting, use the `no ip ospf priority` command.

Parameters

number	Enter a number as the priority. The range is from 0 to 255. The default is **1**.

Defaults

1

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

Setting a priority of 0 makes the router ineligible for election as a designated router or backup designated router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

ip ospf retransmit-interval

Set the retransmission time between lost link state advertisements (LSAs) for adjacencies belonging to the interface.

C9000 Series

Syntax

`ip ospf retransmit-interval seconds`

To return to the default values, use the `no ip ospf retransmit-interval` command.

Parameters

seconds	Enter the number of seconds as the interval between retransmission. The range is from 1 to 3600. The default is **5 seconds**. This interval must be greater than the expected round-trip time for a packet to travel between two routers.

Defaults

5 seconds

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

Set the time interval to a number large enough to prevent unnecessary retransmissions. For example, the interval must be larger for interfaces connected to virtual links.

ip ospf transmit-delay

To send a link state update packet on the interface, set the estimated time elapsed.

C9000 Series

Syntax `ip ospf transmit-delay seconds`

To return to the default value, use the `no ip ospf transmit-delay` command.

Parameters

seconds	Enter the number of seconds as the interval between retransmission. The range is from 1 to 3600. The default is **1 second**. This value must be greater than the transmission and propagation delays for the interface.

Defaults **1 second**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

log-adjacency-changes

To send a Syslog message about changes in the OSPF adjacency state, set the system.

C9000 Series

Syntax `log-adjacency-changes`

To disable the Syslog messages, use the `no log-adjacency-changes` command.

Defaults Disabled.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

maximum-paths

Enable the software to forward packets over multiple paths.

C9000 Series

Syntax `maximum-paths` *number*

To disable packet forwarding over multiple paths, use the `no maximum-paths` command.

Parameters

number	Specify the number of paths. The range for OSPFv2 is from 1 to 64. The default for OSPFv2 is **4 paths**. The range for OSPFv3 is from 1 to 64. The default for OSPFv3 is **8 paths**.

Defaults **4**

Command Modes ROUTER OSPF for OSPFv2

ROUTER OSPFv3 for OSPFv3

Command History This guide is platform-specific. For command information about other platforms, see relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

network area

Define which interfaces run OSPF and the OSPF area for those interfaces.

C9000 Series

Syntax

`network ip-address mask area area-id`

To disable an OSPF area, use the `no network ip-address mask area area-id` command.

Parameters

ip-address	Specify a primary or secondary address in dotted decimal format. The primary address is required before adding the secondary address.
mask	Enter a network mask in /prefix format. (/x)
area-id	Enter the OSPF area ID as either a decimal value or in a valid IP address. Decimal value range is from 0 to 65535. IP address format is dotted decimal format A.B.C.D.

NOTE: If the area ID is smaller than 65535, it is converted to a decimal value. For example, if you use an area ID of 0.0.0.1, it is converted to 1.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.8.1.0	Introduced to all platforms.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

To enable OSPF on an interface, the `network area` command must include, in its range of addresses, the primary IP address of an interface.

NOTE: An interface can be attached only to a single OSPF area.

If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0.

passive-interface

Suppress both receiving and sending routing updates on an interface.

C9000 Series

Syntax

`passive-interface {default | interface}`

To enable both the receiving and sending routing, use the `no passive-interface interface` command.

To return all OSPF interfaces (current and future) to active, use the `no passive-interface default` command.

Parameters

default	Enter the keyword `default` to make all OSPF interfaces (current and future) passive.
interface	Enter the following keywords and slot/port or number information: • For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Modified to include the keyword `default`.
6.1.1.1	Introduced on the E-Series.

Usage Information

Although the passive interface does not send or receive routing updates, the network on that interface is still included in OSPF updates sent using other interfaces.

The `default` keyword sets all interfaces as passive. You can then configure individual interfaces, where adjacencies are desired, using the `no passive-interface` *`interface`* command. The `no` form of this command is inserted into the configuration for individual interfaces when the `no passive-interface` *`interface`* command is issued while `passive-interface default` is configured.

This command behavior has changed as follows:

`passive-interface` *`interface`*

- The previous `no passive-interface` *`interface`* is removed from the running configuration.
- The ABR status for the router is updated.
- Save `passive-interface` *`interface`* into the running configuration.

`passive-interface default`

- All present and future OSPF interfaces are marked as *passive*.
- Any adjacency is explicitly terminated from all OSPF interfaces.
- All previous `passive-interface` *`interface`* commands are removed from the running configuration.
- All previous `no passive-interface` *`interface`* commands are removed from the running configuration.

`no passive-interface` *`interface`*

- Remove the interface from the passive list.
- The ABR status for the router is updated.
- If `passive-interface default` is specified, then save `no passive-interface` *`interface`* into the running configuration.

`No passive-interface default`

- Clear everything and revert to the default behavior.
- All previously marked passive interfaces are removed.
- May update ABR status.

redistribute

Redistribute information from another routing protocol throughout the OSPF process.

C9000 Series

Syntax

`redistribute {connected | rip | static} [metric` *`metric-value`* `| metric-type` *`type-value`*`] [route-map` *`map-name`*`] [tag` *`tag-value`*`]`

To disable redistribution, use the `no redistribute {connected | isis | rip | static}` command.

Parameters

connected	Enter the keyword `connected` to specify that information from active routes on interfaces is redistributed.
rip	Enter the keyword `rip` to specify that RIP routing information is redistributed.
static	Enter the keyword `static` to specify that information from static routes is redistributed.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number. The range is from 0 (zero) to 16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then one of the following: • 1 = OSPF External type 1 • 2 = OSPF External type 2
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of the route map.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` then a number. The range is from 0 to 4294967295.

Defaults

Not configured.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.1	Introduced on the E-Series.

Usage Information To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.

Related Commands default-information originate — generates a default route into the OSPF routing domain.

redistribute bgp

Redistribute BGP routing information throughout the OSPF instance.

C9000 Series

Syntax `redistribute bgp as number [metric metric-value] | [metric-type type-value] | [tag tag-value]`

To disable redistribution, use the `no redistribute bgp as number [metric metric-value] | [metric-type type-value] [route-map map-name] [tag tag-value]` command.

Parameters

as number	Enter the autonomous system number. The range is from 1 to 65535.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then the metric-value number. The range is from 0 to16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then one of the following: • 1 = for OSPF External type 1 • 2 = for OSPF External type 2
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of the route map.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPF. The range is from 0 to 4294967295.

Defaults none

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.8.1.3	Added Route Map for BGP Redistribution to OSPF.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the keyword `default`.
6.1.1.1	Introduced on the E-Series.

redistribute isis

Redistribute IS-IS routing information throughout the OSPF instance.

C9000 Series

Syntax

`redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]`

To disable redistribution, use the `no redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value | metric-type type-value] [route-map map-name] [tag tag-value]` command.

Parameters

tag	(OPTIONAL) Enter the name of the IS-IS routing process.
level-1	(OPTIONAL) Enter the keywords `level-1` to redistribute only IS-IS Level-1 routes.
level-1-2	(OPTIONAL) Enter the keywords `level-1-2` to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keywords `level-2` to redistribute only IS-IS Level-2 routes.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number. The range is from 0 (zero) to 4294967295.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then one of the following: • 1 = for OSPF External type 1 • 2 = for OSPF External type 2
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of the route map.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPF. The range is from 0 to 4294967295.

Defaults Not configured.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

router-id

To configure a fixed router ID, use this command.

C9000 Series

Syntax `router-id ip-address`

To remove the fixed router ID, use the `no router-id ip-address` command.

Parameters

ip-address	Enter the router ID in the IP address format.

Defaults none.

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.1	Introduced on the E-Series.

Usage Information

You can configure an arbitrary value in the IP address format for each router. However, each router ID must be unique. If you use this command on an OSPF router process, which is already active (that is, has neighbors), a prompt reminding you that changing the router-id brings down the existing OSPF adjacency. The new router ID is effective at the next reload.

Example

```
Dell(conf)#router ospf 100
Dell(conf-router_ospf)#router-id 1.1.1.1
Changing router-id will bring down existing OSPF adjacency [y/n]:

Dell(conf-router_ospf)#show config
!
router ospf 100
router-id 1.1.1.1
Dell(conf-router_ospf)#no router-id
Changing router-id will bring down existing OSPF adjacency [y/n]:
Dell#
```

router ospf

To configure an OSPF instance, enter ROUTER OSPF mode.

C9000 Series

Syntax

`router ospf` *process-id* `[vrf {`*vrf name*`}]`

To delete an OSPF instance, use the `no router ospf process-id` command.

Parameters

process-id	Enter a number for the OSPF instance. The range is from 1 to 65535.
vrf-name	Enter the VRF process identifier to tie the OSPF instance to the VRF. All network commands under this OSPF instance are then tied to the VRF instance.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for OSPFv3 on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.9.1.0	Added support for VRF on E-Series.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

You must have an IP address assigned to an interface to enter ROUTER OSPF mode and configure OSPF.

After the OSPF process and the VRF are tied together, you cannot use the OSPF Process ID again in the system. You can only create one process per VRF.

Example

```
To create an OSPF instance in default vrf
Dell(conf)#router ospf 1
Dell(conf-router_ospf-1)#

To create an OSPF instance in a non-default vrf, for example, "vrf1"
Dell(conf)#router ospf 2 vrf vrf1
Dell(conf-router_ospf-2)#
```

show config

Display the non-default values in the current OSPF configuration.

C9000 Series

Syntax `show config`

Command Modes ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell(conf-router_ospf)#show config
!
router ospf 3
passive-interface FastEthernet 0/1
Dell(conf-router_ospf)#
```

show ip ospf

Display information on the OSPF process configured on the switch.

C9000 Series

Syntax `show ip ospf process-id [vrf vrf name]`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view only the OSPF information tied to the VRF process.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Added output for LSA throttling timers.
8.3.7.0	Introduced on the S4810.
7.9.1.0	Added support for VRF on E-Series.
7.8.1.0	Added support of Multi-Process OSPF.
7.8.1.0	Added the *process-id* option, in support of Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information If you delete all the network area commands for Area 0, the `show ip ospf` command output does not list Area 0.

The following describes the `show ip ospf` command shown in the following example.

Line Beginning with	Description
"Routing Process..."	Displays the OSPF process ID and the IP address associated with the process ID.
"Supports only..."	Displays the number of Type of Service (TOS) rouse supported.
"SPF schedule..."	Displays the delay and hold time configured for this process ID.
"Convergence Level"	
"Min LSA...."	Displays the intervals set for LSA transmission and acceptance.
"Number of..."	Displays the number and type of areas configured for this process ID.

Example

```
Dell#show ip ospf 10
Routing Process ospf 10 with ID 1.1.1.1 Virtual router default
Supports only single TOS (TOS0) routes
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Convergence Level 0
Min LSA origination 0 msec, Min LSA arrival 1000 msec
Min LSA hold time 5000 msec, Max LSA wait time 5000 msec
Number of area in this router is 1, normal 1 stub 0 nssa 0
    Area BACKBONE (0)
      Number of interface in this area is 1
      SPF algorithm executed 205 times
      Area ranges are
Dell#
```

Related Commands show ip ospf database — displays information about the OSPF routes configured.

show ip ospf interface — displays the OSPF interfaces configured.

show ip ospf neighbor — displays the OSPF neighbors configured.

show ip ospf asbr

Display all autonomous system boundary router (ASBR) routers visible to OSPF.

C9000 Series

Syntax `show ip ospf process-id | vrf vrf-name asbr`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view all ASBR routers visible to the OSPF process that is tied to a specific VRF.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support of Multi-Process OSPF.
7.8.1.0	Added the *process-id* option, in support of Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information

To isolate problems with external routes, use this command. In OSPF, external routes are calculated by adding the LSA cost to the cost of reaching the ASBR router. If an external route does not have the correct cost, use this command to determine if the path to the originating router is correct. The display output is not sorted in any order.

NOTE: ASBRs that are not in directly connected areas are also displayed.

You can determine if an ASBR is in a directly connected area (or not) by the flags. For ASBRs in a directly connected area, E flags are set. In the following example, router 1.1.1.1 is in a directly connected area since the Flag is E/-/-/. For remote ASBRs, the E flag is clear (-/-/-/).

Example

```
Dell#show ip ospf 1asbr

RouterID  Flags   Cost Nexthop   Interface Area
3.3.3.3   -/-/-/  2    10.0.0.2  Te 0/1    1
1.1.1.1   E/-/-/  0    0.0.0.0   -         0
Dell#
```

show ip ospf database

Display all LSA information. If you do not enable OSPF on the switch, no output is generated.

C9000 Series

Syntax

```
show ip ospf process-id [vrf vrf-name] database [database-summary]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and then the name of the VRF to view LSA information on OSPF processes corresponding to that VRF.
database-summary	(OPTIONAL) Enter the keywords `database-summary` to the display the number of LSA types in each area and the total number of LSAs.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support of Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf` *process-id* `database` command shown in the following example.

Field	Description
Link ID	Identifies the router ID.
ADV Router	Identifies the advertising router's ID.
Age	Displays the link state age.
Seq#	Identifies the link state sequence number. This number allows you to identify old or duplicate link state advertisements.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Link count	Displays the number of interfaces for that router.

Example

```
Dell>show ip ospf 1 database

     OSPF Router with ID (11.1.2.1) (Process ID 1)
                 Router (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       Checksum Link count
```

```
11.1.2.1     11.1.2.1     673  0x80000005 0x707e   2
13.1.1.1     13.1.1.1     676  0x80000097 0x1035   2
192.68.135.2 192.68.135.2 1419 0x80000294 0x9cbd   1

               Network (Area 0.0.0.0)
Link ID      ADV Router   Age  Seq#       Checksum
10.2.3.2     13.1.1.1     676  0x80000003 0x6592
10.2.4.2     192.68.135.2 908  0x80000055 0x683e

               Type-5 AS External
Link ID      ADV Router   Age  Seq#       Checksum Tag
0.0.0.0      192.68.135.2 908  0x80000052 0xeb83   100
1.1.1.1      192.68.135.2 908  0x8000002a 0xbd27   0
10.1.1.0     11.1.2.1     718  0x80000002 0x9012   0
10.1.2.0     11.1.2.1     718  0x80000002 0x851c   0
10.2.2.0     11.1.2.1     718  0x80000002 0x7927   0
10.2.3.0     11.1.2.1     718  0x80000002 0x6e31   0
10.2.4.0     13.1.1.1     1184 0x80000068 0x45db   0
11.1.1.0     11.1.2.1     718  0x80000002 0x831e   0
11.1.2.0     11.1.2.1     718  0x80000002 0x7828   0
12.1.2.0     192.68.135.2 1663 0x80000054 0xd8d6   0
13.1.1.0     13.1.1.1     1192 0x8000006b 0x2718   0
13.1.2.0     13.1.1.1     1184 0x8000006b 0x1c22   0
172.16.1.0   13.1.1.1     148  0x8000006d 0x533b   0
Dell>
```

Related Commands show ip ospf database asbr-summary — displays only ASBR summary LSA information.

show ip ospf database asbr-summary

Display information about autonomous system (AS) boundary LSAs.

C9000 Series

Syntax

```
show ip ospf [process-id |vrf vrf-name] database asbr-summary [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view information about AS boundary LSAs corresponding to a specific VRF.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf database asbr-summary` command shown in the following example.

Field	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric	Displays the LSA metric.

Example

```
Dell#show ip ospf 100 database asbr-summary

     OSPF Router with ID (1.1.1.10) (Process ID 100)

       Summary Asbr (Area 0.0.0.0)
```

```
LS age: 1437
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 103.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x8000000f
Checksum: 0x8221
Length: 28
Network Mask: /0
      TOS: 0 Metric: 2

LS age: 473
Options: (No TOS-capability, No DC, E)
LS type: Summary Asbr
Link State ID: 104.1.50.1
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000010
Checksum: 0x4198
Length: 28
--More--
```

Related Commands show ip ospf database — displays OSPF database information.

show ip ospf database external

Display information on the AS external (type 5) LSAs.

C9000 Series

Syntax

```
show ip ospf [process-id | vrf vrf-name ] database external [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view information on AS external LSAs corresponding to the OSPF processes that are tied to a specific VRF.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information The following describes the `show ip ospf` *`process-id`* `database external` command shown in the following example.

Field	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of the LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
Metrics Type	Displays the external type.
TOS	Displays the Type of Service (TOS) options. Option 0 is the only option.
Metric	Displays the LSA metric.
Forward Address	Identifies the address of the forwarding router. Data traffic is forwarded to this router. If the forwarding address is 0.0.0.0, data traffic is forwarded to the originating router.
External Route Tag	Displays the 32-bit field attached to each external route. The OSPF protocol does not use this field, but you can use the field for external route management.

Example

```
Dell#show ip ospf 1 database external

    OSPF Router with ID (20.20.20.5) (Process ID 1)

         Type-5 AS External

LS age: 612
Options: (No TOS-capability, No DC, E)
LS type: Type-5 AS External
Link State ID: 12.12.12.2
Advertising Router: 20.31.3.1
LS Seq Number: 0x80000007
Checksum: 0x4cde
Length: 36
Network Mask: /32
     Metrics Type: 2
     TOS: 0
     Metrics: 25
     Forward Address: 0.0.0.0
     External Route Tag: 43

LS age: 1868
Options: (No TOS-capability, DC)
LS type: Type-5 AS External
Link State ID: 24.216.12.0
Advertising Router: 20.20.20.8
LS Seq Number: 0x80000005
Checksum: 0xa00e
Length: 36
Network Mask: /24
     Metrics Type: 2
     TOS: 0
     Metrics: 1
     Forward Address: 0.0.0.0
     External Route Tag: 701
Dell#
```

Related Commands show ip ospf database — displays OSPF database information.

show ip ospf database network

Display the network (type 2) LSA information.

C9000 Series

Syntax

```
show ip ospf [process-id | vrf vrf-name] database network [link-state-id] [adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view the network LSA information corresponding to an OSPF process that is tied to a specific VRF
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs

- the default destination (0.0.0.0) for Type 5 LSAs

adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf` *`process-id`* `database network` command shown in the following example.

Field	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
Checksum	Identifies the link state sequence number. This number enables you to identify old or duplicate LSAs.
Length	Displays the Fletcher checksum of an LSA's complete contents.

Field	Description
Network Mask	Displays the length in bytes of the LSA.
Attached Router	Identifies the IP address of routers attached to the network.

Example

```
Dell#show ip ospf 1 data network

    OSPF Router with ID (20.20.20.5) (Process ID 1)

        Network (Area 0.0.0.0)
 LS age: 1372
Options: (No TOS-capability, DC, E)
LS type: Network
Link State ID: 202.10.10.2
Advertising Router: 20.20.20.8
LS Seq Number: 0x80000006
Checksum: 0xa35
Length: 36
Network Mask: /24
     Attached Router: 20.20.20.8
     Attached Router: 20.20.20.9
     Attached Router: 20.20.20.7

         Network (Area 0.0.0.1)

LS age: 252
Options: (TOS-capability, No DC, E)
LS type: Network
Link State ID: 192.10.10.2
Advertising Router: 192.10.10.2
LS Seq Number: 0x80000007
Checksum: 0x4309
Length: 36
Network Mask: /24
     Attached Router: 192.10.10.2
     Attached Router: 20.20.20.1
     Attached Router: 20.20.20.5
Dell#
```

Related Commands show ip ospf database — displays OSPF database information.

show ip ospf database nssa-external

Display NSSA-External (type 7) LSA information.

C9000 Series

Syntax

```
show ip ospf [process-id { vrf vrf-name] database nssa-external [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to view a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword vrf followeed by the name of the VRF to view NSSA-External LSA information corresponding to the OSPF process that is tied to a specific VRF.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

- the network's IP address for Type 3 LSAs or Type 5 LSAs
- the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related Commands show ip ospf database — displays OSPF database information.

show ip ospf database opaque-area

Display the opaque-area (type 10) LSA information.

C9000 Series

Syntax

```
show ip ospf [process-id| vrf vrf-name ] database opaque-area [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view opaque-area LSA information corresponding to the OSPF process that is tied to a specific VRF.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

- the network's IP address for Type 3 LSAs or Type 5 LSAs
- the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

adv-router *ip-address* (OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf` *`process-id`* `database opaque-area` command shown in the following example.

Item	Description
LS Age	Displays the LSA's age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA's type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the advertising router's ID.
Checksum	Displays the Fletcher checksum of the LSA's complete contents.

Item	Description
Length	Displays the length in bytes of the LSA.
Opaque Type	Displays the Opaque type field (the first 8 bits of the Link State ID).
Opaque ID	Displays the Opaque type-specific ID (the remaining 24 bits of the Link State ID).

Example

```
Dell>show ip ospf 1 database opaque-area

    OSPF Router with ID (3.3.3.3) (Process ID 1)
         Type-10 Opaque Link Area (Area 0)

LS age: 1133
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.1
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000416
Checksum: 0x376
Length: 28
Opaque Type: 1
Opaque ID: 1
Unable to display opaque data

LS age: 833
Options: (No TOS-capability, No DC, E)
LS type: Type-10 Opaque Link Area
Link State ID: 1.0.0.2
Advertising Router: 10.16.1.160
LS Seq Number: 0x80000002
Checksum: 0x19c2
--More--
```

Related Commands show ip ospf database — displays OSPF database information.

show ip ospf database opaque-as

Display the opaque-as (type 11) LSA information.

C9000 Series

Syntax

```
show ip ospf [process-id | vrf vrf-name] database opaque-as [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view LSA information tied to the specific VRF.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs

	adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` and the ip-address to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related Commands show ip ospf database — displays OSPF database information.

show ip ospf database opaque-link

Display the opaque-link (type 9) LSA information.

C9000 Series

Syntax

```
show ip ospf [process-id| vrf vrf-name] database opaque-link [link-state-id]
[adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view opaque-link LSA information corresponding to the OSPF process that is tied to a specific VRF.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs

- the default destination (0.0.0.0) for Type 5 LSAs

adv-router *ip-address* (OPTIONAL) Enter the keywords `adv-router` then the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related Commands show ip ospf database — displays OSPF database information.

show ip ospf database router

Display the router (type 1) LSA information.

C9000 Series

Syntax

```
show ip ospf [process-id| vrf vrf-name]database router [link-state-id] [adv-router ip-address]
```

Parameters

process-id Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

vrf *vrf-name* Enter the keyword `vrf` and the name of the VRF to view the router LSA information corresponding to the OSPF process that is tied to a specific VRF.

link-state-id (OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following:

- the network's IP address for Type 3 LSAs or Type 5 LSAs

- the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs
- the default destination (0.0.0.0) for Type 5 LSAs

adv-router *ip-address* (OPTIONAL) Enter the keywords `adv-router` followed by the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf` *`process-id`* `database router` command shown in the following example.

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Displays the link state sequence number. This number detects duplicate or old LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.

Item	Description
Length	Displays the length in bytes of the LSA.
Number of Links	Displays the number of active links to the type of router (Area Border Router or AS Boundary Router) listed in the previous line.
Link connected to:	Identifies the type of network to which the router is connected.
(Link ID)	Identifies the link type and address.
(Link Data)	Identifies the router interface address.
Number of TOS Metric	Lists the number of TOS metrics.
TOS 0 Metric	Lists the number of TOS 0 metrics.

Example

```
Dell#show ip ospf 100 database router

     OSPF Router with ID (1.1.1.10) (Process ID 100)

         Router (Area 0)

LS age: 967
Options: (No TOS-capability, No DC, E)
LS type: Router
Link State ID: 1.1.1.10
Advertising Router: 1.1.1.10
LS Seq Number: 0x8000012f
Checksum: 0x3357
Length: 144
AS Boundary Router
Area Border Router
  Number of Links: 10

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.129.1
    (Link Data) Router Interface address: 192.68.129.1
    Number of TOS metric: 0
       TOS 0 Metric: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.130.1
    (Link Data) Router Interface address: 192.68.130.1
    Number of TOS metric: 0
       TOS 0 Metric: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.142.2
    (Link Data) Router Interface address: 192.68.142.2
    Number of TOS metric: 0
       TOS 0 Metric: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.141.2
    (Link Data) Router Interface address: 192.68.141.2
    Number of TOS metric: 0
       TOS 0 Metric: 1

  Link connected to: a Transit Network
    (Link ID) Designated Router address: 192.68.140.2
    (Link Data) Router Interface address: 192.68.140.2
    Number of TOS metric: 0
       TOS 0 Metric: 1

Link connected to: a Stub Network
```

```
    (Link ID) Network/subnet number: 11.1.5.0
--More--
```

Related Commands show ip ospf database — displays OSPF database information.

show ip ospf database summary

Display the network summary (type 3) LSA routing information.

C9000 Series

Syntax

```
show ip ospf [process-id|vrf vrf-name]database summary [link-state-id] [adv-router ip-address]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view LSA routing information corresponding to the OSPF process that is tied to a specific VRF.
link-state-id	(OPTIONAL) Specify LSA ID in dotted decimal format. The LSA ID value depends on the LSA type, and it can be one of the following: • the network's IP address for Type 3 LSAs or Type 5 LSAs • the router's OSPF router ID for Type 1 LSAs or Type 4 LSAs • the default destination (0.0.0.0) for Type 5 LSAs
adv-router *ip-address*	(OPTIONAL) Enter the keywords `adv-router` then the IP address of an Advertising Router to display only the LSA information about that router.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information The following describes the `show ip ospf process-id database summary` command shown in the following example.

Item	Description
LS Age	Displays the LSA age.
Options	Displays the optional capabilities available on router. The following options can be found in this item: • TOS-capability or No TOS-capability is displayed depending on whether the router can support Type of Service. • DC or No DC is displayed depending on whether the originating router can support OSPF over demand circuits. • E or No E is displayed on whether the originating router can accept AS External LSAs.
LS Type	Displays the LSA type.
Link State ID	Displays the Link State ID.
Advertising Router	Identifies the router ID of the LSA's originating router.
LS Seq Number	Displays the link state sequence number. This number allows you to identify old or duplicate LSAs.
Checksum	Displays the Fletcher checksum of an LSA's complete contents.
Length	Displays the length in bytes of the LSA.
Network Mask	Displays the network mask implemented on the area.
TOS	Displays the TOS options. Option 0 is the only option.
Metric	Displays the LSA metrics.

Example

```
Dell#show ip ospf 100 database summary

    OSPF Router with ID (1.1.1.10) (Process ID 100)

        Summary Network (Area 0.0.0.0)

LS age: 1551
Options: (No TOS-capability, DC, E)
LS type: Summary Network
Link State ID: 192.68.16.0
Advertising Router: 192.168.17.1
LS Seq Number: 0x80000054
Checksum: 0xb5a2
Length: 28
Network Mask: /24
    TOS: 0 Metric: 1

LS age: 9
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.32.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x987c
Length: 28
```

```
Network Mask: /24
   TOS: 0 Metric: 1

LS age: 7
Options: (No TOS-capability, No DC, E)
LS type: Summary Network
Link State ID: 192.68.33.0
Advertising Router: 1.1.1.10
LS Seq Number: 0x80000016
Checksum: 0x1241
Length: 28
Network Mask: /26
   TOS: 0 Metric: 1
```

Related Commands show ip ospf database — displays OSPF database information.

show ip ospf interface

Display the OSPF interfaces configured. If OSPF is not enabled on the switch, no output is generated.

C9000 Series

Syntax `show ip ospf [process-id | vrf vrf-name] interface [interface]`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view the OSPF processes that are tied to a specific VRF.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For the null interface, enter the keyword `null` then zero (0). • For loopback interfaces, enter the keyword `loopback` then a number from 0 to 16383. • For tunnel interfaces, enter the keyword `tunnel` then a number from 0 to 16383. • For Port Channel groups, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094. • For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf` *`process-id`* `interface` command shown in the following example.

Item	Description
TenGigabitEthernet...	This line identifies the interface type slot/port and the status of the OSPF protocol on that interface.
Internet Address...	This line displays the IP address, network mask and area assigned to this interface.
Process ID...	This line displays the OSPF Process ID, Router ID, Network type and cost metric for this interface.
Transmit Delay...	This line displays the interface's settings for Transmit Delay, State, and Priority. In the State setting, BDR is Backup Designated Router.
Designated Router...	This line displays the ID of the Designated Router and its interface address.
Backup Designated...	This line displays the ID of the Backup Designated Router and its interface address.
Timer intervals...	This line displays the interface's timer settings for Hello interval, Dead interval, Transmit Delay (Wait), and Retransmit Interval.
Hello due...	This line displays the amount time until the next Hello packet is sent out this interface.
Neighbor Count...	This line displays the number of neighbors and adjacent neighbors. Listed below this line are the details about each adjacent neighbor.

Example

```
Dell>show ip ospf int

TenGigabitEthernet 1/17 is up, line protocol is up
  Internet Address 192.168.1.2/30, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 192.168.253.2, Interface address 192.168.1.2
  Backup Designated Router (ID) 192.168.253.1, Interface address 192.168.1.1
```

```
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:02
  Neighbor Count is 1, Adjacent neighbor count is 1
    Adjacent with neighbor 192.168.253.1 (Backup Designated Router)

TenGigabitEthernet 1/23 is up, line protocol is up
  Internet Address 192.168.0.1/24, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DROTHER, Priority 1
  Designated Router (ID) 192.168.253.5, Interface address 192.168.0.4
  Backup Designated Router (ID) 192.168.253.3, Interface address 192.168.0.2
  Timer intervals configured, Hello 10, Dead 40, Wait 40, Retransmit 5
    Hello due in 00:00:08
  Neighbor Count is 3, Adjacent neighbor count is 2
    Adjacent with neighbor 192.168.253.5 (Designated Router)
    Adjacent with neighbor 192.168.253.3 (Backup Designated Router)

Loopback 0 is up, line protocol is up
  Internet Address 192.168.253.2/32, Area 0.0.0.1
  Process ID 1, Router ID 192.168.253.2, Network Type LOOPBACK, Cost: 1
Loopback interface is treated as a stub Host.
Dell>
```

show ip ospf neighbor

Display the OSPF neighbors connected to the local router.

C9000 Series

Syntax `show ip ospf [process-id |vrf vrf-name] neighbor`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view information corresponding to the OSPF neighbors that are tied to a specific VRF.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information The following describes the `show ip ospf process-id neighbor` command shown in the following example.

Item	Description
Neighbor ID	Displays the neighbor router ID.
Pri	Displays the priority assigned neighbor.
State	Displays the OSPF state of the neighbor.
Dead Time	Displays the expected time until the system declares the neighbor dead.
Address	Displays the IP address of the neighbor.
Interface	Displays the interface type slot/port information.
Area	Displays the neighbor's area (process ID).

Example

```
Dell#show ip ospf 34 neighbor

Neighbor ID Pri State       Dead Time Address  Interface Area
20.20.20.7  1 FULL/DR     00:00:32 182.10.10.3 Te 0/0 0.0.0.2
192.10.10.2 1 FULL/DR     00:00:37 192.10.10.2 Te 0/1 0.0.0.1
20.20.20.1  1 FULL/DROTHER00:00:36 192.10.10.4 Te 0/1 0.0.0.1
Dell#
```

show ip ospf routes

Display routes OSPF calculates and stores in OSPF RIB.

C9000 Series

Syntax `show ip ospf [process-id|vrf vrf-name]routes`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view the OSPF RIB information corresponding to the OSPF processes that are tied to a specific VRF.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information

This command is useful in isolating routing problems between the OSPF and the RTM. For example, if a route is missing from the RTM/FIB but is visible from the display output of this command, the problem is with downloading the route to the RTM.

This command has the following limitations:

- The display output is sorted by prefixes; intra-area ECMP routes are not displayed together.
- For Type 2 external routes, Type 1 cost is not displayed.

Example

```
Dell#show ip ospf 100 route

Prefix         Cost Nexthop    Interface Area  Type
1.1.1.1         1   0.0.0.0    Lo 0      0     Intra-Area
3.3.3.3         2   13.0.0.3   Te 0/47   1     Intra-Area
13.0.0.0        1   0.0.0.0    Te 0/47   0     Intra-Area
150.150.150.0   2   13.0.0.3   Te 0/47   -     External
172.30.1.0      2   13.0.0.3   Te 0/47   1     Intra-Area
Dell#
```

show ip ospf statistics

Display OSPF statistics.

C9000 Series

Syntax

```
show ip ospf [process-id | vrf vrf-name] statistics global | [interface name
{neighbor router-id}]
```

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to display statistics corresponding to the OSPF process that is tied to a specific VRF.
global	Enter the keyword `global` to display the packet counts received on all running OSPF interfaces and packet counts OSPF neighbors receive and transmit.

interface *name*

(OPTIONAL) Enter the keyword `interface` then one of the following interface keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` then a number.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

neighbor *router-id*

(OPTIONAL) Enter the keyword `neighbor` then the neighbor's router-id in dotted decimal format (A.B.C.D.).

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.9.1.0	Added support for VRF on E-Series.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ip ospf statistics` *`process-id`* `global` command shown in the following example.

Row Heading	Description
Total	Displays the total number of packets the OSPF process receives/transmits.
Error	Displays the error count while receiving and transmitting packets by the OSPF process.
Hello	Number of OSPF Hello packets.
DDiscr	Number of database description packets.
LSReq	Number of link state request packets.
LSUpd	Number of link state update packets.
LSAck	Number of link state acknowledgement packets.
TxQ-Len	The transmission queue length.
RxQ-Len	The reception queue length.
Tx-Mark	The highest number mark in the transmission queue.
Rx-Mark	The highest number mark in the reception queue.
Hello-Q	The queue, for transmission or reception, for the hello packets.
LSR-Q	The queue, for transmission or reception, for the link state request packets.
Other-Q	The queue, for transmission or reception, for the link state acknowledgement, database description, and update packets.

The following describes the error definitions for the `show ip ospf statistics` *`process-id`* `global` command.

Error Type	Description
Intf_Down	Received packets on an interface that is either down or OSPF is not enabled.
Non-Dr	Received packets with a destination address of ALL_DRS even though SELF is not a designated router.
Self-Org	Receive the self originated packet.
Wrong_Len	The received packet length is different to what was indicated in the OSPF header.
Invld-Nbr	LSA, LSR, LSU, and DDB are received from a peer which is not a neighbor peer.
Nbr-State	LSA, LSR, and LSU are received from a neighbor with stats less than the loading state.
Auth-Error	Simple authentication error.
MD5-Error	MD5 error
Cksum-Err	Checksum Error
Version	Version mismatch
AreaMismatch	Area mismatch
Conf-Issue	The received hello packet has a different hello or dead interval than the configuration.
No-Buffer	Buffer allocation failure.
Seq-no	A sequence no errors occurred during the database exchange process.
Socket	Socket Read/Write operation error.
Q-overflow	Packets dropped due to queue overflow.
Unknown-Pkt	Received packet is not an OSPF packet.

Error Type	Description
RtidZero	Received router-ID (0.0.0.0) from peer.

Example

```
ell#show ip ospf 1 statistics
Interface TenGigabitEthernet 0/0
  Error packets (Receive statistics)
     Intf-Down           0   Non-Dr                0   Self-Org            0
     Wrong-Len           0   Invld-Nbr             0   Nbr-State           0
     Auth-Error          0   MD5-Error             0   Cksum-Err           0
     Version             0   AreaMisMatch          0   Conf-Issue          0
     SeqNo-Err           0   Unknown-Pkt           0   Bad-LsReq           0
     RtidZero            0
  Neighbor ID 1.2.1.1
     Packet Statistics
                Hello    DDiscr     LSReq     LSUpd     LSAck
        RX        130         2         1         3         3
        TX        144         2         1         3         2
     Timers
        Hello     6  Wait         0  Grace     0
        Dead     38  Transmit     0
     Queue Statistics
        LSU-Q-Len           0  LSU-Q-Wmark             2
        LSR-Q-Len           0  LSR-Q-Wmark             1
```

```
Dell#show ip ospf 1 statistics global

 OSPF Packet Count
         Total      Error      Hello      DDiscr     LSReq      LSUpd      LSAck
RX         114          0        105          2          1          3          3
TX         127          0        119          2          1          3          2

 OSPF Global Queue Length
                TxQ-Len    RxQ-Len    Tx-Mark    Rx-Mark
    Hello-Q           0          0          0          0
    LSR-Q             0          0          0          0
    Other-Q           0          0          0          0

 Error packets (Receive statistics)
Intf-Down           0   Non-Dr                0   Self-Org            0
Wrong-Len           0   Invld-Nbr             0   Nbr-State           0
Auth-Err            0   MD5-Err               0   Chksum              0
Version             0   AreaMis               0   Conf-Issues         0
No-Buffer           0   Seq-No                0   Socket              0
Q-OverFlow          0   Unknown-Pkt           0   RtidZero            0

 Error packets (Transmit statistics)
Socket Errors          0
```

Usage Information

The `show ip ospf` *process-id* `statistics` command displays the error packet count received on each interface as:

- The hello-timer remaining value for each interface
- The wait-timer remaining value for each interface
- The grace-timer remaining value for each interface
- The packet count received and transmitted for each neighbor
- Dead timer remaining value for each neighbor
- Transmit timer remaining value for each neighbor
- The LSU Q length and its highest mark for each neighbor
- The LSR Q length and its highest mark for each neighbor

Example (Statistics)

```
Dell#show ip ospf 100 statistics

Interface TenGigabitEthernet 0/8

  Hello-Timer 9, Wait-Timer 0, Grace-Timer 0
  Error packets (Only for RX)
```

```
Intf-Down   0  Non-Dr        0  Self-Org     0
Wrong-Len   0  Invld-Nbr     0  Nbr-State    0
Auth-Error  0  MD5-Error     0  Cksum-Err    0
Version     0  AreaMisMatch  0  Conf-Issue   0
SeqNo-Err   0  Unkown-Pkt    0

  Neighbor ID 9.1.1.2

     Hello DDiscr LSReq LSUpd LSAck
RX   59    3      1     1     1
TX   62    2      1     0     0

  Dead-Timer  37, Transmit-Timer  0
  LSU-Q-Len    0, LSU-Q-Wmark     0
  LSR-Q-Len    0, LSR-Q-Wmark     1
```

Related Commands clear ip ospf statistics — clears the packet statistics in all interfaces and neighbors.

show ip ospf timers rate-limit

Show the LSA currently in the queue waiting for timers to expire.

C9000 Series

Syntax `show ip ospf [process-id|vrf vrf-name]timers rate-limit`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view LSAs corresponding to a specific VRF that are currently in queue waiting for timers to expire.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show ip ospf 10 timers rate-limit

List of LSAs in rate limit Queue
LSA id: 1.1.1.0 Type: 3 Adv Rtid: 3.3.3.3 Expiry time: 00:00:09.111
LSA id: 3.3.3.3 Type: 1 Adv Rtid: 3.3.3.3 Expiry time: 00:00:23.96
Dell#
```

show ip ospf topology

Display routers in directly connected areas.

C9000 Series

Syntax `show ip ospf [process-id| vrf vrf-name] topology`

Parameters

process-id	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
vrf *vrf-name*	Enter the keyword `vrf` and the name of the VRF to view the information on routers corresponding to a specific VRF that are in directly connected areas.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.4(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series and E-Series.

Usage Information To isolate problems with inter-area and external routes, use this command. In OSPF inter-area and external routes are calculated by adding LSA cost to the cost of reaching the router. If an inter-area or external route is not of correct cost, the display can determine if the path to the originating router is correct or not.

Example

```
Dell#show ip ospf 1 topology

Router ID  Flags Cost  Nexthop   Interface Area
3.3.3.3    E/B/-/ 1    20.0.0.3  Te 13/1   0
1.1.1.1    E/-/-/ 1    10.0.0.1  Te 7/1    1
Dell#
```

summary-address

To advertise one external route, set the OSPF ASBR.

C9000 Series

Syntax

`summary-address` *ip-address mask* `[not-advertise] [tag` *tag-value*`]`

To disable summary address, use the `no summary-address` *ip-address mask* command.

Parameters

ip-address	Specify the IP address in dotted decimal format of the address to summarize.
mask	Specify the mask in dotted decimal format of the address to summarize.
not-advertise	(OPTIONAL) Enter the keywords `not-advertise` to suppress that match the network prefix/mask pair.
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` then a value to match on routes redistributed through a route map. The range is from 0 to 4294967295.

Defaults

Not configured.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

The `area range` command summarizes routes for the different areas.

With the `not-advertise` parameter configured, you can use this command to filter out some external routes. For example, if you want to redistribute static routes to OSPF, but you don't want OSPF to advertise routes with prefix 1.1.0.0, you can configure the summary-address 1.1.0.0 255.255.0.0 not-advertise to filter out all the routes fall in range 1.1.0.0/16.

Related Commands area range — summarizes routes within an area.

timers spf

Set the time interval between when the switch receives a topology change and starts a shortest path first (SPF) calculation.

Syntax `timers spf delay holdtime`

To return to the default, use the `no timers spf` command.

Parameters

delay	Enter a number as the delay. The range is from 0 to 4294967295. The default is **5 seconds**.
holdtime	Enter a number as the hold time. The range is from 0 to 4294967295. The default is **10 seconds**.

Defaults

- delay = 5 seconds
- holdtime = 10 seconds

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
pre-6.1.1.1	Introduced on the E-Series.

Usage Information Setting the *delay* and *holdtime* parameters to a low number enables the switch to an alternate path quickly but requires more CPU usage.

Example

```
Dell# conf
Dell(conf)# router ospf 1
Dell(conf-router_ospf-1)# timer spf 2 5
Dell(conf-router_ospf-1)# show config
!
router ospf 1
timers spf 2 5
Dell(conf-router_ospf-1)# end
```

timers throttle lsa all

Configure LSA transmit intervals.

C9000 Series

Syntax `timers throttle lsa all {start-interval | hold-interval | max-interval}`

To return to the default, use the `no timers throttle lsa` command.

Parameters

start-interval	Set the minimum interval between initial sending and resending the same LSA. The range is from 0 to 600,000 milliseconds.
hold-interval	Set the next interval to send the same LSA. This interval is the time between sending the same LSA after the start-interval has been attempted. The range is from 1 to 600,000 milliseconds.
max-interval	Set the maximum amount of time the system waits before sending the LSA. The range is from 1 to 600,000 milliseconds.

Defaults

- start-interval: **0 msec**
- hold-interval: **5000 msec**
- max-interval: **5000 msec**

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Usage Information LSAs are sent after the start-interval and then after hold-interval until the maximum interval is reached. In throttling, exponential backoff is used when sending same LSA, so that the interval is multiplied until the maximum time is reached. For example, if the *start-interval 5000* and *hold-interval 1000* and *max-interval 100,000*, the LSA is sent at 5000 msec, then 1000 msec, then 2000 msec, them 4000 until 100,000 msec is reached.

timers throttle lsa arrival

Configure the LSA acceptance intervals.

C9000 Series

Syntax `timers throttle lsa arrival` *`arrival-time`*

To return to the default, use the `no timers throttle lsa` command.

Parameters

arrival-time	Set the interval between receiving the same LSA repeatedly, to allow sufficient time for the system to accept the LSA. The range is from 0 to 600,000 milliseconds.

Defaults **1000 msec**

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

OSPFv3 Commands

The fundamental mechanisms of OSPF (flooding, DR election, area support, SPF calculations, and so on) remain unchanged. However, OSPFv3 runs on a per-link basis instead of on a per-IP-subnet basis. Most changes were necessary to handle the increased address size of IPv6.

The Dell Networking implementation of OSPFv3 is based on IETF RFC 2740.

area authentication

Configure an IPsec authentication policy for OSPFv3 packets in an OFSPFv3 area.

C9000 Series

Syntax

```
area area-id authentication ipsec spi number {MD5 | SHA1} [key-encryption-type] key
```

Parameters

area *area-id*	Area for which OSPFv3 traffic is to be authenticated. For area-id, you can enter a number. The range is from 0 to 4294967295.
ipsec spi *number*	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
MD5 | SHA1	Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
key-encryption-type	(OPTIONAL) Specifies if the key is encrypted. The values are 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

Defaults

Not configured.

Command Modes

ROUTER OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
8.4.2.0	Introduced on the E-Series TeraScale.

Usage Information

Before you enable IPsec authentication on an OSPFv3 area, you must first enable OSPFv3 globally on the router. Configure the same authentication policy (same SPI and key) on each interface in an OSPFv3 link.

An SPI number must be unique to one IPsec security policy (authentication or encryption) on the router.

If you have enabled IPsec encryption in an OSPFv3 area with the `area encryption` command, you cannot use the `area authentication` command in the area at the same time.

The configuration of IPsec authentication on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area authentication policy that has been configured is applied to the interface.

To remove an IPsec authentication policy from an OSPFv3 area, enter the `no area area-id authentication spi number` command.

Related Commands

ipv6 ospf authentication – configures an IPsec authentication policy on an OSPFv3 interface.

show crypto ipsec policy – displays the configuration of IPsec authentication policies.

area encryption

Configure an IPsec encryption policy for OSPFv3 packets in an OSPFv3 area.

C9000 Series

Syntax

```
area area-id encryption ipsec spi number esp encryption-algorithm [key-encryption-type] key authentication-algorithm [key-encryption-type] key
```

Parameters

area *area-id*	Area for which OSPFv3 traffic is to be encrypted. For *area-id*, enter a number. The range is from 0 to 4294967295.
ipsec spi *number*	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
esp encryption-algorithm	Encryption algorithm used with ESP. Valid values are: 3DES, DES, AES-CBC, and NULL. For AES-CBC, only the AES-128 and AES-192 ciphers are supported.
key-encryption-algorithm	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in encryption. The required lengths of a non-encrypted or encrypted key are:

	3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC -32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.
authentication-algorithm	Specifies the authentication algorithm to use for encryption. Valid values are `MD5` or `SHA1`.
key-encryption-type	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).
null	Causes an encryption policy configured for the area to not be inherited on the interface.

Defaults Not configured.

Command Modes ROUTER OSPFv3

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.4.2.0	Introduced on the E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information Before you enable IPsec encryption on an OSPFv3 interface, first enable OSPFv3 globally on the router. Configure the same encryption policy (same SPI and keys) on each interface in an OSPFv3 link.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router.

When you configure encryption for an OSPFv3 area with the `area encryption` command, you enable both IPsec encryption and authentication. However, when you enable authentication on an area with the `area authentication` command, you do not enable encryption at the same time.

If you have enabled IPsec authentication in an OSPFv3 area with the `area authentication` command, you cannot use the `area encryption` command in the area at the same time.

The configuration of IPsec encryption on an interface-level takes precedence over an area-level configuration. If you remove an interface configuration, an area encryption policy that has been configured is applied to the interface.

To remove an IPsec encryption policy from an interface, enter the no area *area-id* encryption spi *number* command.

Related Commands

ipv6 ospf encryption – configures an IPsec encryption policy on an OSPFv3 interface.

show crypto ipsec policy – display the configuration of IPsec encryption policies.

area nssa

Specify an area as a not so stubby area (NSSA).

Syntax

```
area area-id nssa [default-information-originate] [no-redistribution] [no-summary]
```

To delete an NSSA, use the `no area area-id nssa` command.

Parameters

area-id	Specify the OSPF area by entering a number from zero (0) to 65535.
no-redistribution	(OPTIONAL) Specify that the `redistribute` command does not distribute routes into the NSSA. This command can be used when the router is an autonomous system boundary router (ASBR) or area border router (ABR).
default-information-originate	(OPTIONAL) Allows external routing information to be imported into the NSSA by using Type 7 default.
no-summary	(OPTIONAL) Specify that no summary LSAs should be sent into the NSSA.

Defaults

Not configured.

Command Modes

ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13(0.0)	Introduced on the remaining DNOS platforms.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.

Version	Description
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for the Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre- 6.1.1.1	Introduced on the E-Series.

auto-cost

Specify how the OSPF interface cost is calculated based on the reference bandwidth method.

C9000 Series

Syntax

`auto-cost [reference-bandwidth ref-bw]`

To return to the default bandwidth or to assign cost based on the interface type, use the `no auto-cost [reference-bandwidth]` command.

Parameters

ref-bw	(OPTIONAL) Specify a reference bandwidth in megabits per second. The range is from 1 to 4294967. The default is **100 megabits per second**.

Defaults

100 megabits per second.

Command Modes

ROUTER OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

clear ipv6 ospf process

Reset an OSPFv3 router process without removing or re-configuring the process.

C9000 Series

Syntax

`clear ipv6 ospf [vrf vrf-name] process`

Parameters

vrf *vrf-name*	(Optional) Enter the keyword vrf and the name of the VRF to clear IPv6 routes corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on the E-Series.

clear ipv6 route

Clear (refresh) all or a specific route from the IPv6 routing table.

C9000 Series

Syntax `clear ipv6 route {* | ipv6-address prefix-length }[vrf vrf-name]`

Parameters

*	Enter the * to clear (refresh) all routes from the IPv6 routing table.
ipv6-address prefix-length	Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
vrf *vrf-name*	(Optional) Enter the keyword vrf and the name of the VRF to clear the IPv6 routes corresponding to that VRF.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Added support for VRF.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

debug ipv6 ospf bfd

Display debug information and interface types for bidirectional forwarding detection (BFD) on OSPF IPv6 packets.

C9000 Series

Syntax `[no] debug ipv6 ospf bfd [interface]`

Parameters

interface (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a tunnel interface, enter the keyword `tunnel` then a number. The range is from 1 to 16383.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Introduced on the S4820T, S4810, and Z9000.

Usage Information The following section describes the command fields.

Lines Beginning With or Including	Description
OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.
05:21:01	Displays the time stamp.
Sending Ver:3	Sending OSPF3 version..

Example

```
Dell(conf-if-te-0/2)#do debug ipv6 ospf bfd te 0/2
OSPFv3 bfd related debugging is on for TenGigabitEthernet 0/2
00:59:26 : OSPFv3INFO: Received Interface mode bfd config command on interface
Te 0/2 Enable 1, interval 0, min_rx 0, Multiplier 0, role 0, Disable 0
00:59:26 : OSPFv3INFO: Enabling BFD on interface Te 0/2 Cmd Add Session
00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720
00:59:27 : OSPFv3INFO: Completed Enabling BFD on interface Te 0/2
00:59:27 : OSPFv3INFO: Completed Interface mode BFD configuration on Te 0/2!!
00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720
00:59:27 : OSPFv3INFO: Ospf3_register_bfd ospf key 27648
00:59:27 : OSPFv3INFO: OSPFV3 Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720 Interface Te 0/2 IfIndex 34145282
00:59:27 : OSPFv3INFO: BFD parameters interval 100 min_rx 100 mult 3 role
active
00:59:27 : OSPFv3INFO: BFD parameters interval 100 min_rx 100 mult 3 role
active
00:59:27 : OSPFv3INFO: Completed Enabling BFD for NBRIP
fe80:0000:0000:0000:0201:e8ff:fe8b:7720
Aug 25 11:19:59: %STKUNIT0-M:CP %BFDMGR-1-BFD_STATE_CHANGE: Changed session
state to Init for neighbor fe80::201:e8ff:fe8b:7720 on interface Te 0/2 (diag:
NBR_DN)
Aug 25 11:20:00: %STKUNIT0-M:CP %BFDMGR-1-BFD_STATE_CHANGE: Changed session
state to Up for neighbor fe80::201:e8ff:fe8b:7720 on interface Te 0/2 (diag:
NO_DIAG)
00:59:45 : OSPFv3INFO: OSPFV3 got BFD msg
00:59:45 : OSPFv3INFO: Bfd Msg Type Up for interface Te 0/2
00:59:45 : OSPFv3INFO: OSPFV3 updating NBR state
```

debug ipv6 ospf events

Display debug information and interface types on OSPF IPv6 events.

Syntax `debug ipv6 ospf events [interface] [vrf vrf-name]`

Parameters

interface (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

vrf *vrf-name*	Enter the keyword `vrf` to view debugging information on OSPF corresponding to that VRF.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on E-Series.

Example

Example (detail)

Command Fields

Lines Beginning With or Including	Description
OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.
05:21:01	Displays the time stamp.
Sending Ver:3	Sending OSPF3 version..
type:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
Length:	Displays the OSPFv3 packet length.
Router ID:	Displays the OSPFv3 router ID.
Area ID:	Displays the OSPFv3 area ID.
Chksum:	Displays the OSPFv3 checksum.

debug ipv6 ospf packet

Display debug information and interface types on OSPF IPv6 packets.

Syntax `debug ipv6 ospf packet [interface] [vrf vrf-name] [detail]`

Parameters

interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
vrf *vrf-name*	Enter the keyword `vrf` to view debugging information on OSPF corresponding to that VRF.
detail	Enter the keyword `detail` to view detailed debugging information.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13(0.0)	Added support for detailed debugging.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on E-Series.

Example

Example (detail)

Command Fields

Lines Beginning With or Including	Description
OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.
05:21:01	Displays the time stamp.
Sending Ver:3	Sending OSPF3 version..
type:	Displays the type of packet sent: • 1 - Hello packet • 2 - database description • 3 - link state request • 4 - link state update • 5 - link state acknowledgement
Length:	Displays the OSPFv3 packet length.
Router ID:	Displays the OSPFv3 router ID.
Area ID:	Displays the OSPFv3 area ID.
Chksum:	Displays the OSPFv3 checksum.

debug ipv6 ospf spf

Display debug information for SPF timers on OSPF IPv6 packets.

Syntax `[no] debug ipv6 ospf spf`

Parameters

interface	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a port channel interface, enter the keywords `port-channel` then a number. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11.0.0	Introduced the command.

Usage Information The following section describes the command fields.

Lines Beginning With or Including	Description
OSPFv3...	Debugging is on for all OSPFv3 packets and all interfaces.
05:21:01	Displays the time stamp.
Sending Ver:3	Sending OSPF3 version..

Example

default-information originate

Configure the system to generate a default external route into an OSPFv3 routing domain.

C9000 Series

Syntax

`default-information originate [always] [metric` *`metric-value`*`] [metric-type` *`type-value`*`] [route-map` *`map-name`*`]`

To return to the default values, use the `no default-information originate` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to specify that default route information must always be advertised.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number to configure a metric value for the route. The range is from 1 to 16777214.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then an OSPFv3 link state type of 1 or 2 for default routes. The values are: • 1 = Type 1 external route • 2 = Type 2 external route
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map.

Defaults

Disabled.

Command Modes

ROUTER OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.

Version	Description
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands redistribute — redistributes routes from other routing protocols into OSPFv3.

graceful-restart grace-period

Enable OSPFv3 graceful restart globally by setting the grace period (in seconds) that an OSPFv3 router's neighbors continues to advertise the router as adjacent during a graceful restart.

C9000 Series

Syntax `graceful-restart grace-period` *seconds*

To disable OSPFv3 graceful restart, enter `no graceful-restart grace-period`.

Parameters

seconds	Time duration, in seconds, that specifies the duration of the restart process before OSPFv3 terminates the process. The range is from 40 to 1800 seconds.

Defaults OSPFv3 graceful restart is disabled and functions in a helper-only role.

Command Modes ROUTER OSPFv3

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.4.2.2	Introduced on the E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA.

To enable OSPFv3 graceful restart, enter the ipv6 router ospf command to enter OSPFv3 configuration mode and then configure a grace period using the graceful-restart grace-period command. The grace period is the length of time that OSPFv3 neighbors continue to advertise the restarting router as though it is fully adjacent. When graceful restart is enabled (restarting role), an OSPFv3 restarting expects its OSPFv3 neighbors to help when it restarts by not advertising the broken link.

When you enable the helper-reject role on an interface with the ipv6 ospf graceful-restart helper-reject command, you reconfigure OSPFv3 graceful restart to function in a “restarting-only” role. In a “restarting-only” role, OSPFv3 does not participate in the graceful restart of a neighbor.

graceful-restart mode

Specify the type of events that trigger an OSPFv3 graceful restart.

C9000 Series

Syntax

```
graceful-restart mode {planned-only | unplanned-only}
```

To disable graceful restart mode, enter `no graceful-restart mode`.

Parameters

planned-only	(OPTIONAL) Enter the keywords `planned-only` to indicate graceful restart is supported in a planned restart condition only.
unplanned-only	(OPTIONAL) Enter the keywords `unplanned-only` to indicate graceful restart is supported in an unplanned restart condition only.

Defaults

OSPFv3 graceful restart supports both planned and unplanned failures.

Command Modes

ROUTER OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.4.2.2	Introduced on the E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information

OSPFv3 graceful restart supports planned-only and/or unplanned-only restarts. The default is support for both planned and unplanned restarts.

- A planned restart occurs when you enter the `redundancy force-failover rpm` command to force the primary RPM to switch to the backup RPM. During a planned restart, OSPF sends out a Type-11 Grace LSA before the system switches over to the backup RPM.
- An unplanned restart occurs when an unplanned event causes the active RPM to switch to the backup RPM, such as when an active process crashes, the active RPM is removed, or a power failure happens. During an unplanned restart, OSPF sends out a Grace LSA when the backup RPM comes online.

By default, both planned and unplanned restarts trigger an OSPFv3 graceful restart. Selecting one or the other mode restricts OSPFv3 to the single selected mode.

ipv6 neighbor

Configure a static entry in the IPv6 neighbor discovery.

C9000 Series

Syntax

`ipv6 neighbor{ipv6-address} {interface interface} {hardware_address}[vrf vrf-name]`

To remove a static IPv6 entry from the IPv6 neighbor discovery, use the `no ipv6 neighbor ipv6-address{interface interface`

Parameters

ipv6-address Enter the IPv6 address of the neighbor in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zero.

interface *intehardware_rface* Enter the keyword `interface` then the interface type and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port/subport information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a Null interface, enter the keyword null then the Null interface number.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel interface number. The range is from 1 to 16383.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is from 1 to 48
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

hardware_address Enter a 48-bit hardware MAC address in nn:nn:nn:nn:nn:nn format.

vrf *vrf-name* (Optional) Enter the keyword vrf and the name of the VRF to install IPv6 routes in that VRF.

Defaults none

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

Usage Information

Neighbor Discovery Protocol for IPv6 is defined in RFC 2461 as part of the Stateless Address Autoconfiguration protocol. It replaces the Address Resolution Protocol used with IPv4. It defines mechanisms for solving problems, such as:

- Router discovery: Hosts can locate routers residing on a link
- Prefix discovery: Hosts can discover address prefixes for the link.
- Parameter discovery
- Address autoconfiguration — configuration of addresses for an interface
- Address resolution — mapping from IP address to link-layer address
- Next-hop determination· Neighbor Unreachability Detection (NUD): Determine that a neighbor is no longer reachable on the link
- Duplicate Address Detection (DAD): Allow a node to check whether a proposed address is already in use.
- Redirect: The router can inform a node about a better first-hop.

Use the ipv6 neighbor command to manually configure the IPv6 address of a neighbor to be discovered by the switch.

NOTE: The parameters vrf, mac-address, interface are not supported in the batch mode.

ipv6 ospf area

Enable IPv6 OSPF on an interface.

C9000 Series

Syntax

`ipv6 ospf` *`process id`* `area`*`area id`*

To disable OSPFv6 routing for an interface, use the `no ipv6 ospf` *`process-id`* `area` *`area-id`* command.

Parameters

process-id	Enter the process identification number.
area *area-id*	Specify the OSPF area. The range is from 0 to 4294967295.

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.14(0.2)	Increased the area ID value from 65535 to 4294967295.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.4.1.0	Introduced on the E-Series and C-Series.

ipv6 ospf authentication

Configure an IPsec authentication policy for OSPFv3 packets on an IPv6 interface.

C9000 Series

Syntax `ipv6 ospf authentication {null | ipsec spi number {MD5 | SHA1} [key-encryption-type] key}}`

Parameters

null	Causes an authentication policy configured for the area to not be inherited on the interface.
ipsec spi number	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
MD5 | SHA1	Authentication type: Message Digest 5 (MD5) or Secure Hash Algorithm 1 (SHA-1).
key-encryption-type	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted).

For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on S4810 and Z9000.
8.4.2.0	Introduced on the E-Series.
8.3.19.0	Introduced on the S4820T.

Usage Information Before you enable IPsec authentication on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same authentication policy (same SPI and key) on each OSPFv3 interface in a link.

To remove an IPsec authentication policy from an interface, enter the no ipv6 ospf authentication `spi` *`number`* command. To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, enter the `no ipv6 ospf authentication null` command.

Related Commands area authentication – configures an IPsec authentication policy for an OSPFv3 area.

show crypto ipsec policy – displays the configuration of IPsec authentication policies.

show crypto ipsec sa ipv6 – displays the security associations set up for OSPFv3 interfaces in authentication policies.

ipv6 ospf bfd all-neighbors

Establish BFD sessions with all OSPFv3 neighbors on a single interface or use non-default BFD session parameters.

C9000 Series

Syntax `ipv6 ospf bfd all-neighbors [disable | [interval` *`interval`* `min_rx` *`min_rx`* `multiplier` *`value`* `role {active | passive}]]`

To disable all BFD sessions on an OSPFv3 interface implicitly, use the `no ipv6 ospf bfd all-neighbors disable` command in interface mode..

Parameters

disable	(OPTIONAL) Enter the keyword `disable` to disable BFD on this interface.
interval *milliseconds*	(OPTIONAL) Enter the keyword `interval` to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is **200**.
min_rx *milliseconds*	Enter the keywords `min_rx` to specify the minimum rate at which the local system receives control packets from the remote system. The range is from 50 to 1000. The default is **200**.
multiplier *value*	Enter the keyword `multiplier` to specify the number of packets that must be missed in order to declare a session down. The range is from 3 to 50. The default is **3**.
role [active | passive]	Enter the role that the local system assumes: • `Active` — The active system initiates the BFD session. Both systems can be active for the same session. • `Passive` — The passive system does not initiate a session. It only responds to a request for session initialization from the active system. The default is **Active**.

Defaults See Parameters

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2.0.0	Introduced on the Z9000, S4820T, and S4810.

Usage Information This command provides the flexibility to fine-tune the timer values based on individual interface needs when you configure ipv6 ospf BFD in CONFIGURATION mode. Any timer values specified with this command overrides timers set using the `bfd all-neighbors` command. Using the `no` form of this command does not disable BFD if you configure BFD in CONFIGURATION mode.

To disable BFD on a specific interface while you configure BFD in CONFIGURATION mode, use the keyword `disable`.

ipv6 ospf cost

Explicitly specify the cost of sending a packet on an interface.

C9000 Series

Syntax `ipv6 ospf` *interface-cost*

Parameters

interface-cost	Enter a unsigned integer value expressed as the link-state metric. The range is from 1 to 65535.

Defaults Default cost based on the bandwidth.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on the E-Series.
8.3.19.0	Introduced on the S4820T.

Usage Information In general, the path cost is calculated as:

10^8 / bandwidth

Using this formula, the default path cost is calculated as:

- 10-Gigabit Ethernet—Default cost is 1
- 40-Gigabit Ethernet — Default cost is 1

ipv6 ospf dead-interval

Set the time interval since the last hello-packet was received from a router. After the time interval elapses, the neighboring routers declare the router down.

C9000 Series

Syntax `ipv6 ospf dead-interval` *seconds*

To return to the default time interval, use the `no ipv6 ospf dead-interval` command.

Parameters

seconds	Enter the time interval in seconds. The range is from 1 to 65535 seconds.

Defaults 40 seconds (Ethernet).

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
7.8.1.0	Added support for C-Series.
7.4.1.0	Introduced on the E-Series.
8.3.19.0	Introduced on the S4820T.

Usage Information

By default, the dead interval is four times longer than the default hello-interval.

Related Commands

ipv6 ospf hello-interval – specifies the time interval between hello packets.

ipv6 ospf encryption

Configure an IPsec encryption policy for OSPFv3 packets on an IPv6 interface.

C9000 Series

Syntax

```
ipv6 ospf encryption {null | ipsec spi number esp encryption-algorithm [key-encryption-type] key athentication-algorithm [key-encryption-type] key}}
```

Parameters

null	Causes an encryption policy configured for the area to not be inherited on the interface.
ipsec spi number	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
esp *encryption-algorithm*	Encryption algorithm used with ESP. Valid values are: 3DES, DES, AES-CBC, and NULL. For AES-CBC, only the AES-128 and AES-192 ciphers are supported.
key-encryption-type	(OPTIONAL) Specifies if the key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. The required lengths of a non-encrypted or encrypted key are:

	3DES - 48 or 96 hex digits; DES - 16 or 32 hex digits; AES-CBC -32 or 64 hex digits for AES-128 and 48 or 96 hex digits for AES-192.
authentication-algorithm	Specifies the authentication algorithm to use for encryption. Valid values are `MD5` or `SHA1`.
key-encryption-type	(OPTIONAL) Specifies if the authentication key is encrypted. Valid values: 0 (key is not encrypted) or 7 (key is encrypted).
key	Text string used in authentication. For MD5 authentication, the key must be 32 hex digits (non-encrypted) or 64 hex digits (encrypted). For SHA-1 authentication, the key must be 40 hex digits (non-encrypted) or 80 hex digits (encrypted).

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.4.2.0	Introduced on the E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information Before you enable IPsec encryption on an OSPFv3 interface, first enable IPv6 unicast routing globally, configure an IPv6 address and enable OSPFv3 on the interface, and assign the interface to an area.

An SPI value must be unique to one IPsec security policy (authentication or encryption) on the router. Configure the same encryption policy (same SPI and key) on each OSPFv3 interface in a link.

To remove an IPsec encryption policy from an interface, enter the `no ipv6 ospf encryption spi` *`number`* command. To remove null authentication on an interface to allow the interface to inherit the authentication policy configured for the OSPFv3 area, enter the `no ipv6 ospf no ipv6 ospf encryption null` command.

Related Commands area encryption – configures an IPsec encryption policy for an OSPFv3 area.

show crypto ipsec policy – displays the configuration of IPsec encryption policies.

show crypto ipsec sa ipv6 – displays the security associations set up for OSPFv3 interfaces in encryption policies.

ipv6 ospf graceful-restart helper-reject

Configure an OSPFv3 interface to not act upon the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

C9000 Series

Syntax

`ipv6 ospf graceful-restart helper-reject`

To disable the helper-reject role, enter `no ipv6 ospf graceful-restart helper-reject`.

Defaults

The helper-reject role is not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.4.2.2	Introduced on E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information

By default, OSPFv3 graceful restart is disabled and functions only in a helper role to help restarting neighbor routers in their graceful restarts when it receives a Grace LSA.

When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

The graceful-restart role command is not supported in OSPFv3. When you enable the helper-reject role on an interface, you reconfigure an OSPFv3 router to function in a “restarting-only” role.

ipv6 ospf hello-interval

Specify the time interval between the hello packets sent on the interface.

C9000 Series

Syntax

`ipv6 ospf hello–interval` *`seconds`*

To return to the default time interval, enter `no ipv6 ospf hello–interval`.

Parameters

seconds	Enter the time interval in seconds as the time between hello packets. The range is from 1 to 65525 seconds.

Defaults 10 seconds (Ethernet).

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.
8.3.19.0	Introduced on the S4820T.

Usage Information The time interval between hello packets must be the same for routers in a network.

Related Commands ipv6 ospf dead-interval – specifies the time interval between hello packets was received from a router.

ipv6 ospf priority

To determine the Designated Router for the OSPFv3 network, set the priority of the interface.

C9000 Series

Syntax `ipv6 ospf priority number`

To return to the default time interval, use the `no ipv6 ospf priority` command.

Parameters

number	Enter the number as the priority. The range is from 1 to 255.

Defaults 1

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

Setting a priority of 0 makes the router ineligible for election as a Designated Router or Backup Designated Router.

Use this command for interfaces connected to multi-access networks, not point-to-point networks.

ipv6 router ospf

Enable OSPF for IPv6 router configuration.

C9000 Series

Syntax

`ipv6 router ospf` *process-id* `[vrf` *vrf-name*`]`

To exit OSPF for IPv6, use the `no ipv6 router ospf` *process-id* command.

Parameters

process-id	Enter the process identification number. The range is from 1 to 65535.
vrf *vrf-name*	(Optional) Enter the keyword vrf and the name of the VRF to install IPv6 routes in that VRF.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.

Version	Description
7.4.1.0	Introduced on the E-Series.

maximum-paths

Enable the software to forward packets over multiple paths.

C9000 Series

Syntax `maximum-paths` *number*

To disable packet forwarding over multiple paths, use the `no maximum-paths` command.

Parameters

number	Specify the number of paths. The range is from 1 to 64. The default is **8** paths.

Defaults 8

Command Modes ROUTER OSPF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Added support for Multi-Process OSPF.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

passive-interface

Disable (suppress) sending routing updates on an interface.

C9000 Series

Syntax `passive—interface` *interface*

To enable sending routing updates on an interface, use the `no passive-interface` *interface* command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Enabled, that is sending of routing updates are enabled by default.

Command Modes ROUTER OSPF for OSPFv2

ROUTER OSPFv3 for OSPFv3

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information By default, no interfaces are *passive*. Routing updates are sent to all interfaces on which the routing protocol is enabled.

If you disable the sending of routing updates on an interface, the particular address prefix continues to be advertised to other interfaces, and updates from other routers on that interface continue to be received and processed.

OSPFv3 for IPv6 routing information is not sent or received through the specified router interface. The specified interface address appears as a stub network in the OSPFv3 for IPv6 domain.

redistribute

Redistribute into OSPFv3.

C9000 Series

Syntax

`redistribute {bgp` *`as number`*`}{connected | static}[metric` *`metric-value`* `| metric-type` *`type-value`*`] [route-map` *`map-name`*`] [tag` *`tag-value`*`]`

To disable redistribution, use the `no redistribute {connected | static}` command.

Parameters

bgp *as number*	Enter the keyword `bgp` then the autonomous system number. The range is from 1 to 65535.
connected	Enter the keyword `connected` to redistribute routes from physically connected interfaces.
static	Enter the keyword `static` to redistribute manually configured routes.
metric *metric-value*	Enter the keyword `metric` then the metric value. The range is from 0 to 16777214. The default is **20**.
metric-type *type-value*	(OPTIONAL) Enter the keywords `metric-type` then the OSPFv3 link state type of 1 or 2 for default routes. The values are: • 1 for a type 1 external route • 2 for a type 2 external route The default is **2**.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of an established route map. If the route map is not configured, the default is **deny** (to drop all routes).
tag *tag-value*	(OPTIONAL) Enter the keyword `tag` to set the tag for routes redistributed into OSPFv3. The range is from 0 to 4294967295 The default is **0**.

Defaults

Not configured.

Command Modes

ROUTER OSPF for OSPFv2

ROUTER OSPFv3 for OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

To redistribute the default route (x:x:x:x::x), use the `default-information originate` command.

Related Commands

default-information originate – configures default external route into OSPFv3.

router-id

Designate a fixed router ID.

C9000 Series

Syntax

`router-id ip-address`

To return to the previous router ID, use the `no router-id ip-address` command.

Parameters

ip-address	Enter the router ID in the dotted decimal format.

Defaults

The router ID is selected automatically from the set of IPv4 addresses configured on a router.

Command Modes

ROUTER OSPF for OSPFv2

ROUTER OSPFv3 for OSPFv3

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.

Version	Description
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

You can configure an arbitrary value in the IP address for each router. However, each router ID must be unique.

If this command is used on an OSPFv3 process that is already active (has neighbors), all the neighbor adjacencies are brought down immediately and new sessions are initiated with the new router ID.

Related Commands

clear ipv6 ospf process – resets an OSPFv3 router process.

show crypto ipsec policy

Display the configuration of IPsec authentication and encryption policies.

C9000 Series

Syntax

```
show crypto ipsec policy [name name]
```

Parameters

name *name*	(OPTIONAL) Displays configuration details about a specified policy.

Defaults

None.

Command Modes

EXEC

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.4.2.0	Introduced on the E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information

The `show crypto ipsec policy` command output displays the AH and ESP parameters configured in IPsec security policies, including the SPI number, keys, and algorithms used.

When configured in a helper-reject role, an OSPFv3 router ignores the Grace LSAs that it receives from a restarting OSPFv3 neighbor.

Table 6. `show crypto ipsec policy` Command Description

Field	Description
Policy name	Displays the name of an IPsec policy.
Policy refcount	Number of interfaces on the router that use the policy
Inbound ESP SPI Outbound ESP SPI	The encapsulating security payload (ESP) security policy index (SPI) for inbound and outbound links.
Inbound ESP Auth Key Outbound ESP Auth Key	The ESP authentication key for inbound and outbound links.
Inbound ESP Cipher Key Outbound ESP Cipher Key	The ESP encryption key for inbound and outbound links.
Transform set	The set of security protocols and algorithms used in the policy.
Inbound AH SPI Outbound AH SPI	The authentication header (AH) security policy index (SPI) for inbound and outbound links.
Inbound AH Key Outbound AH Key	The AH key for inbound and outbound links.

Example

```
Dell#show crypto ipsec policy

Crypto IPSec client security policy data

Policy name : OSPFv3-1-502
Policy refcount : 1
Inbound ESP SPI : 502 (0x1F6)
Outbound ESP SPI : 502 (0x1F6)
Inbound ESP Auth Key : 123456789a123456789b123456789c12
Outbound ESP Auth Key : 123456789a123456789b123456789c12
Inbound ESP Cipher Key :
123456789a123456789b123456789c123456789d12345678
Outbound ESP Cipher Key :
123456789a123456789b123456789c123456789d12345678
Transform set : esp-3des esp-md5-hmac

Crypto IPSec client security policy data

Policy name : OSPFv3-0-501
Policy refcount : 1
Inbound ESP SPI : 501 (0x1F5)
Outbound ESP SPI : 501 (0x1F5)
Inbound ESP Auth Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e97eb7c0
c30808825fb5
Outbound ESP Auth Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba8ed8bb5efe91e97eb7c0
c30808825fb5
Inbound ESP Cipher Key :
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba10345a1039ba8f8a
Outbound ESP Cipher Key :
```

```
bbdd96e6eb4828e2e27bc3f9ff541e43faa759c9ef5706ba10345a1039ba8f8a
Transform set : esp-128-aes esp-sha1-hmac
```

show crypto ipsec sa ipv6

Display the IPsec security associations (SAs) used on OSPFv3 interfaces.

C9000 Series

Syntax `show crypto ipsec sa ipv6 [interface interface]`

Parameters

interface *interface* (OPTIONAL) Displays information about the SAs used on a specified OSPFv3 interface, where *interface* is one of the following values:

- For a Port Channel interface, enter `port-channel number`.
- For a 10-Gigabit Ethernet interface, enter `TenGigabitEthernet slot/port`.
- For a 40–Gigabit Ethernet interface, enter `fortyGigE slot/port`.
- For a VLAN interface, enter `vlan vlan-id`. The valid VLAN IDs range is from 1 to 4094.

Defaults None.

Command Modes EXEC

EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Introduced on the S4810 and Z9000.
8.4.2.0	Introduced on the E-Series TeraScale.
8.3.19.0	Introduced on the S4820T.

Usage Information The `show crypto ipsec sa ipv6` command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.

Example

Table 7. `show crypto ipsec sa ipv6` Command Description

Field	Description
Interface	IPv6 interface.
Link local address	IPv6 address of interface
IPSecv6 policy name	Name of the IPsec security policy applied to the interface.
inbound/outbound ah	Authentication policy applied to inbound or outbound traffic.
inbound/outbound esp	Encryption policy applied to inbound or outbound traffic.
spi	Security policy index number used to identify the policy.
inbound/outbound esp	Encryption policy applied to inbound or outbound traffic.
spi	Security policy index number used to identify the policy.
transform	Security algorithm that is used to provide authentication, integrity, and confidentiality.
in use settings	Transform that the SA uses (only transport mode is supported).
replay detection support	Y: An SA has enabled the replay detection feature. N: The replay detection feature is not enabled.
STATUS	ACTIVE: The authentication or encryption policy is enabled on the interface.

Related Commands

show crypto ipsec policy – displays the configuration of IPsec authentication and encryption policies.

Example

```
Dell#show crypto ipsec policy
Dell#show crypto ipsec sa ipv6

Interface: TenGigabitEthernet 0/0
 Link Local address: fe80::201:e8ff:fe40:4d10
 IPSecv6 policy name: OSPFv3-1-500

 inbound ah sas
  spi : 500 (0x1f4)
   transform : ah-md5-hmac
   in use settings : {Transport, }
   replay detection support : N
   STATUS : ACTIVE

 outbound ah sas
  spi : 500 (0x1f4)
   transform : ah-md5-hmac
   in use settings : {Transport, }
   replay detection support : N
   STATUS : ACTIVE
```

```
 inbound esp sas

 outbound esp sas


Interface: TenGigabitEthernet 0/1
 Link Local address: fe80::201:e8ff:fe40:4d11
 IPSecv6 policy name: OSPFv3-1-600

 inbound ah sas

 outbound ah sas

 inbound esp sas
  spi : 600 (0x258)
   transform : esp-des esp-sha1-hmac
   in use settings : {Transport, }
   replay detection support : N
   STATUS : ACTIVE

 outbound esp sas
  spi : 600 (0x258)
   transform : esp-des esp-sha1-hmac
   in use settings : {Transport, }
   replay detection support : N
   STATUS : ACTIVE
```

show ipv6 ospf interface

View OSPFv3 interface information.

C9000 Series

Syntax

```
show ipv6 ospf [process-number] [vrf vrf-name][interface]
```

Parameters

process-number — Enter the OSPF process number.

vrf *vrf-name* — (OPTIONAL) Enter the keyword vrf and the name of the VRF to display neighbors corresponding to that VRF.

NOTE: If you do not specify this option, neighbors corresponding to the default VRF are displayed.

interface — (OPTIONAL) Enter one of the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` then a number.

- For a tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.2.(0.0)	Added support for showing BFD status on the S4820T, S4810, and Z9000.
9.1.(0.0)	Added support for OSPFv3 on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information If you enable BFD at the global level, *show ipv6 ospf interface* shows the BFD provisioning.

If you enable BFD at the interface level, *show ipv6 ospf interface* shows the BFD interval timers.

Example

```
Dell#show ipv6 ospf 3 interface gigabitethernet 1/2

GigabitEthernet 1/2 is up, line protocol is up
  Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID 67420217
  Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1
  NetworkType BROADCAST, Cost: 1, Passive: No
  Transmit Delay is 100 sec, State DR, Priority 1
  Interface is using OSPF global mode BFD configuration.
  Designated router on this network is 11.1.1.1 (local)
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 1, Retransmit 5

Dell#
```

```
Dell#show ipv6 ospf 3 interface tengigabitethernet 1/2

TenGigabitEthernet 1/2 is up, line protocol is up
  Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID 67420217
  Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1
  NetworkType BROADCAST, Cost: 1, Passive: No
  Transmit Delay is 100 sec, State DR, Priority 1
  Interface is using OSPF global mode BFD configuration.
  Designated router on this network is 11.1.1.1 (local)
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 1, Retransmit 5
```

```
Dell#
```

```
Dell#show ipv6 ospf 3 interface tengigabitethernet 1/2/1

TenGigabitEthernet 1/2/1 is up, line protocol is up
  Link Local Address fe80::201:e8ff:fe17:5bbd, Interface ID 67420217
  Area 0, Process ID 1, Instance ID 0, Router ID 11.1.1.1
  NetworkType BROADCAST, Cost: 1, Passive: No
  Transmit Delay is 100 sec, State DR, Priority 1
  Interface is using OSPF global mode BFD configuration.
  Designated router on this network is 11.1.1.1 (local)
  No backup designated router on this network
  Timer intervals configured, Hello 10, Dead 40, Wait 1, Retransmit 5

Dell#
```

Related Commands show ip ospf interface—Display the OSPF interfaces configured.

show ipv6 ospf database

Display information in the OSPFv3 database, including link-state advertisements (LSAs) in detail.

Syntax

```
show ipv6 ospf [process-number] [vrf vrf-name] database [database-summary | grace-lsa | external | inter-area-prefix | inter-area-router | intra-area-prefix | link | network | router | nssa-external]
```

Parameters

process-number	Enter the OSPF process number.
vrf *vrf-name*	(Optional) Enter the keyword vrf followed by the name of the VRF to display neighbors corresponding to that VRF. **NOTE: If you do not specify this option, neighbors corresponding to the default VRF are displayed.**
database-summary	(OPTIONAL) Enter the keyword `database-summary` to view a summary of database LSA information.
external	(OPTIONAL): Enter the keyword `external` to display the external link states.
grace-lsa	(OPTIONAL): Enter the keyword `grace-lsa` to display the Type-11 Grace LSAs sent and received on an OSPFv3 router.
inter-area-prefix	(OPTIONAL): Enter the keyword `inter-area-prefix` to display the inter area prefix link states.
inter-area-router	(OPTIONAL): Enter the keyword `inter-area-router` to display the inter area router link states.
intra-area-prefix	(OPTIONAL): Enter the keyword `intra-area-prefix` to display the intra area prefix link states.
link	(OPTIONAL): Enter the keyword `link` to display the link states.
network	(OPTIONAL): Enter the keyword `network` to display the network link states.
nssa-external	(OPTIONAL): Enter the keyword `nssa-external` to display the nssa link state information.

router	(OPTIONAL): Enter the keyword `router` to display the router link states.

Defaults None

Command Modes EXEC

EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13(0.0)	Added support to display all the types of LSAs in detail.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100-ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Added support for VRF.
9.2(1.0)	Introduced on the Z9500.
9.1.(0.0)	Added support for OSPFv3 on the S4810 and Z9000.
8.4.2.2	Added support for the display of graceful restart parameters and Type-11 Grace LSAs on E-Series routers.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for C-Series.

Usage Information The `show ipv6 ospf database` command output displays detailed information on the OSPFv3 database, including link-state advertisements (LSAs).

Example (grace-lsa)

Example (database-summary)

Example (external)

```
DellEMC# show ipv6 ospf database external

      OSPFv3 Router with ID (10.160.3.37) (Process ID 6)

                        AS External Link States (Area 0)

  LS Age: 1651
  LS Type: OSPFv3 AS external LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.130.254.101
  LS Seq Number: 0x80000001
  Checksum: 0xF038
  Length: 36
        Prefix: 9001::/64
```

```
        Prefix Options: 0x10 ( DN  )
        Metric Type: 2  Metric: 20
```

Example (nssa-external)

```
DellEMC#show ipv6 ospf 10 database nssa-external

             OSPFv3 Router with ID (1.1.1.1) (Process ID 10)

                    AS External Link States (Area 1)

  LS Age: 35
  LS Type: OSPFv3 NSSA LSA
  Link State ID: 0.0.0.1
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0xD2DD
  Length: 52
       Prefix: 101:101:1::/64
       Prefix Options: 0x8 ( P  )
       Metric Type: 2  Metric: 20
       Forwarding Address: 101:101:1::1
```

show ipv6 ospf neighbor

Display the OSPF neighbor information on a per-interface basis.

C9000 Series

Syntax

```
show ipv6 ospf [process-number] [vrf vrf-name] neighbor [interface]
```

Parameters

process-number — Enter the OSPF process number.

vrf *vrf-name* — (OPTIONAL) Enter the keyword vrf followed by the name of the VRF to display OSPF neighbors corresponding to that VRF.

NOTE: If you do not specify this option, neighbors corresponding to the default VRF are displayed.

interface — (OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a tunnel interface, enter the keyword `tunnel` then the tunnel ID. The range is from 1 to 16383.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults none

Command Modes EXEC

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF on all platforms (Except MXL and STOMP).
9.1.(0.0)	Introduced support for OSPFv3 on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.
7.8.1.0	Added support for the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell#show ipv6 ospf 3 neighbor gi 1/2

Neighbor ID  Pri   State       Dead Time   Interface   ID Interface
63.114.8.36  1   FULL/DR   00:00:38       4              Gi 1/2

Dell#
```

```
Dell#show ipv6 ospf 3 neighbor gi 1/2

Neighbor ID  Pri   State       Dead Time   Interface   ID Interface
63.114.8.36  1   FULL/DR   00:00:38       4              Te 1/2

Dell#
```

```
Dell#show ipv6 ospf 3 neighbor gi 1/2

Neighbor ID  Pri   State       Dead Time   Interface   ID Interface
63.114.8.36  1   FULL/DR   00:00:38       4              Te 1/2/1

Dell#
```

snmp context

Configure SNMPv3 context name to map multiple OSPFv3 VRF instances.

Syntax

`snmp context {context-name}`

To clear snmp context, use the `no snmp context {context-name}` command.

Parameters

context-name	Enter the SNMP context name. The maximum length is 32 alphanumeric characters.

Defaults

None.

Command Modes

IPv6 ROUTER OSPF

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.0)	Introduced on the S3100 series, S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000, S6010–ON, S6100–ON, Z9100–ON, Z9500, S6000–ON, C9010, MXL, and FN IOM.

Usage Information Use SNMPv3 context configuration to distinguish between various OSPFv3 VRF instances.

Example

```
DellEMC(conf-ipv6-router_ospf)#snmp context ospf1
```

```
DellEMC>show runnig-config ospf
!
ipv6 router ospf 10
 router-id 10.10.10.1
 snmp context ospf1
!
DellEMC>
```

40

PE Console Commands

To configure a C1048P port extender from an attached PE console, you can use the following commands. Use these commands when the port extender cannot connect to a C9010.

You can also enter the PE console commands to debug an error condition in a PE stack.

- cd
- clear logging
- copy
- delete
- diag
- dir
- disable
- enable
- exit
- format
- hostname
- offline
- online
- power-cycle
- pwd
- reload
- rename
- reset
- show boot system
- show clock
- show control-bridge status
- show diag
- show diag information
- show diag testcase
- show environment
- show file
- show file-systems
- show interfaces
- show inventory
- show lldp neighbors
- show logging
- show logging driverlog
- show logging kernellog
- show os-version
- show privilege
- show redundancy

- show revision
- show system
- show tech-support
- show version
- telnet-peer-stack-unit

For information about the commands you can enter from a C9010 console to configure a port extender, see Port Extenders (PE) chapter.

Topics:

- diag
- offline
- online
- power-cycle
- show control-bridge status
- show system
- telnet-peer-stack-unit
- upgrade system

diag

Run offline diagnostics on all stack-units.

C9000 Series

Syntax

```
diag {stack-unit unit-number} [alllevels | level0 | level1 | level2]
[interactive] [testname name] [terminate]
```

Parameters

stack-unit *unit-number*	Enter the `stack-unit` value to run offline diagnostic test on a specified stack-unit. The stack-unit range is 0 to 7.
alllevels	Enter the keyword `all levels` to run the complete set of offline diagnostic tests.
level0	Enter the keyword `level0` to run Level 0 diagnostics. Level 0 diagnostics check for the presence of various components and perform essential path verifications. In addition, they verify the identification registers of the components on the board.
level1	Enter the keyword `Level1` to run Level 1 diagnostics. Level 1 diagnostics is a smaller set of diagnostic tests with support for automatic partitioning. They perform status/self test for all the components on the board and test their registers for appropriate values. In addition, they perform extensive tests on memory devices (for example, SDRAM, flash, NVRAM, EEPROM, and CPLD) wherever possible. At this level, ports are shut down automatically.
level2	Enter the keyword `level2` to run Level 2 diagnostics. Level 2 diagnostics are a full set of diagnostic tests with no support for automatic partitioning. Level 2 diagnostics are used primarily for on-board loopback tests and more extensive component diagnostics. Various components on the board are put into Loopback mode and test packets are transmitted through those components. These diagnostics also perform snake tests using VLAN configurations.
interactive	Enter the keyword `interactive` to run offline diagnostics in interactive mode.

NOTE: On a C1048P, interactive diagnostic tests are supported only in standalone mode; they are not supported in stacking mode.

testname *name*	Enter the `testname name` parameters to run a specified offline diagnostic test. Enclose the test-case name in double quotes (" "). For example: `diag level1 testname "first"`.
terminate	Enter the keyword `terminate` to stop the offline diagnostic tests that are running.

Defaults

All offline diagnostic tests are run on all switch CPUs (Control Processor, Route Processor, and line cards).

Command Modes

EXEC Privilege

Usage Information

Before you use this command to run diagnostic test, make sure that the port extender (PE) stack-unit is offline (`offline stack-unit` *`unit number`* command). You are prompted to reboot when the offline diagnostics is complete.

The PE unit goes offline and reboots automatically after the test is completed. Once the test is finished, the diag report is generated, and it is stored in the PE flash. To view the diag report, use the `show diag pe` *`pe-id`* `stack-unit` *`unit-number`* command from C9000 system. The `show diag pe` command uploads the TestReport from the PE to the C9000.

The filename of the TestReport is:`TestReport-SU-Stack-Unit-Number-PE-pe-id-Year_Month_Day_Unique-Tag.txt`, where SU identifies the PE stack-unit on which the offline diag test was run, `Year_Month_Day` is a timestamp to identify when the offline diag test was run for that unit, and the `Unique Tag` is to identify that specific diag test. Diag test reports on PE are not overwritten. Offline diag test reports for PE are stored in the following directory: `flash://default_diag_report_dir`. To view the test report, use the `show file flash://filename` command.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced the `verbose` option.
7.7.1.0	Introduced on the S-Series.

Example

```
Dell#offline stack-unit 3
Warning - offline of unit will bring down all the protocols and
the unit will be operationally down, except for running Diagnostics.
Please make sure that stacking is not configured for Diagnostics execution.
If configured, the unit roles may change. The unit will become standalone once
diags are executed.
Also reboot/online command is necessary for normal operation after the offline
command is issued.
Proceed with Offline [confirm yes/no]:yes
```

```
Dell#diag stack-unit 3 level0
Warning - diagnostic execution will cause multiple link flaps on the peer side
- advisable to shut directly connected ports
Proceed with Diags [confirm yes/no]: yes
```

Related Commands

- offline
- online

offline

Place the PE stack-unit in the offline state to run the diagnostics tests.

C9000 Series

Syntax `offline stack-unit unit-number`

Parameters

stack-unit *slot-id*	Enter the keyword `stack-unit` and specify the stack-unit number. The stack-unit number range is from 0 to 7.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.

Usage Information Use this command to make the port extender offline and run offline diagnostics tests. After this command is issued, a warning message appears cautioning you about bringing down all the protocols and turning down the PE unit operationally during the diagnostics tests. If offline diagnostics are not run after issuing the `offline stack-unit` command, you must issue the `online stack-unit` command to bring up the PE stack-unit.

```
Dell#offline stack-unit 3
Warning - offline of unit will bring down all the protocols and the unit will
be operationally down, except for running Diagnostics. Please make sure that
stacking is not configured for Diagnostics execution. If configured, the unit
roles may change. The unit will become standalone once diags are executed.
Also reboot/online command is necessary for normal operation after the offline
command is issued. Proceed with Offline [confirm yes/no]:
```

Related Commands

- diag — run diagnostic tests on an offline switch.
- online–brings a PE stack-unit back online after running offline diagnostic tests.

online

Bring a PE stack-unit back to an online state after running the offline diagnostics tests.

C9000 Series

Syntax `online stack–unit unit-number`

Parameters

stack-unit *unit-number*	Enter the keyword `stack-unit` and specify the stack-unit number. The stack-unit number range is from 0 to 7.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command-Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C1048P.

Example

```
Dell#diag stack-unit 3 level0 verbose no-reboot
Warning - diagnostic execution will cause multiple link flaps on the peer side
- advisable to shut directly connected ports
Warning - It is highly recommended to reboot the system after Offline
Diagnostics
Proceed with Diags [confirm yes/no]: yes
Dell#Jun 25 05:15:14: %PE-UNKN-C1048P:3 %DIAGAGT-6-DA_DIAG_STARTED: Starting
diags on stack-unit 3
14:19:49 : Approximate time to complete the Diags (level0)... 2 Mins
```

Related Commands

- diag — run diagnostic tests on an offline switch.
- offline — places the stack-unit in the offline state to run the diagnostics tests.

power-cycle

Power-cycle the port extender (PE) stack-unit from the PE console

C9000 Series

Syntax `power-cycle stack-unit {unit-number | all }`

Parameters

unit-number	Enter a stack-unit number. Range is from 0 to 7.
all	Enter `all` to power-cycle all the stack-units.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.

Usage Information

CAUTION: Do not attempt to reset or power cycle when the system is going through the process of upgrading.

Example

```
Dell#power-cycle ?
stack-unit              Stack-unit
Dell#power-cycle stack-unit ?
<0-7>                   Unit number
all                     Entire stack
Dell#power-cycle stack-unit 0

Dell#power-cycle stack-unit all ?
```

show control-bridge status

Display the status of the control bridge from the port extender (PE) console.

C9000 Series

Syntax `show control-bridge status`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command-Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C1048P.

Example

```
Dell#show control-bridge status
Reason: CNU - CSP Not Up, IPE - IPC Program Error
PPE - PEM Program Error, CPE - CHM Program Error
UE - UnKnown Error

CB System MAC : 34:17:eb:00:20:00
Csp Sess Status : UP
Active CB : YES
Uplink LAG : Port-channel 257
LAG Admin Status : UP
LAG Oper Status : UP
```

```
--------------------------------
Status Reason RPM-Id PE-Id
--------------------------------
Online -      0      255
```

Usage Information

Use the `show control-bridge status` command output information to debug the connectivity issues between the control bridge and port extender.

show system

Display the status of a specific stack-unit from the port extender (PE) console.

Syntax

`show system [brief | stack-unit unit-id | stack-ports [status | topology]`

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to view an abbreviated list of system information.
stack-unit *unit-id*	(OPTIONAL) Enter the keywords `stack-unit` then the stack unit number for information. The stack-unit number range is from 0 to 7.
stack-ports *status* | *topology*	(OPTIONAL) Enter the keywords `stack-ports` for information about the status or topology of the stack ports.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Added support for the `disabled-ports` parameter .
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.4	The `brief` parameter no longer displays the current Reload mode. To display Reload mode, use the `show reload-type` command. Modified the `show system stack-unit` command output to support Piece Part ID (PPID).
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	The Boot Flash field displays the code level for boot code 2.8.1.1 and newer, while older boot codes display as "Present".
7.7.1.0	Added Master Priority field.
7.6.1.0	Introduced on the S-Series.

Example (PE Console)

```
Dell#show system stack-unit 1

--  Unit 1 --
Unit Type                  : Management Unit
Status                     : online
Next Boot                  : online
Required Type              : C1048P - 48-port GE (VE)
Current Type               : C1048P - 48-port GE (VE)
Master priority            : 2
Hardware Rev               : 5.0
Num Ports                  : 52
Up Time                    : 2 wk, 0 day, 0 hr, 24 min
Dell Networking OS Version : 1-0(0-4092)
Jumbo Capable              : yes
POE Capable                : yes
FIPS Mode                  : disabled
Boot Flash                 : 3.3.1.7
Boot Selector              : Present
Memory Size                : 1073741824 bytes
Temperature                : 29C
Voltage                    : ok
Serial Number              : NA
Part Number                : 7590009701 Rev 001
Vendor Id                  : NA
Date Code                  : NA
Country Code               : NA
Piece Part ID              : US-0F14T0-77951-3AG-000A
PPID Revision              : 01
Service Tag                : NA
Expr Svc Code              : NA
Auto Reboot                : enabled
Burned In MAC              : 6c:c0:00:43:09:90
No Of MACs                 : 3

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus   FanSpeed(rpm)
--------------------------------------------------------------
  1     0    up           AC      NA          NA
  1     1    absent               NA          NA

--  Fan  Status  --
Unit Bay   TrayStatus  Fan0    Speed   Fan1    Speed
--------------------------------------------------------------
 1    0     up          up      12000   up      12000

Speed in RPM
```

```
ell#show system stack-port status
Topology: Stand alone
Interface  Link Speed       Admin     Link
             (Gb/s)         Status    Status
-----------------------------------------
  1/50         10            up        down
  1/51         10            up        down
```

```
Dell#show system stack-port topology
Topology: Stand alone
Interface  Connection
---------------------
  1/50
  1/51
```

Example (show system stack unit – disabled ports)

Example (show system brief)

Example (S6000)

```
Dell#show system

Stack MAC : 90:b1:1c:f4:9b:79
Reload-Type                :   normal-reload [Next boot : normal-reload]

--  Unit 0 --
Unit Type                  : Management Unit
Status                     : online
Next Boot                  : online
Required Type              : S6000 - 32-port TE/FG (SI)
Current Type               : S6000 - 32-port TE/FG (SI)
Master priority            : 0
Hardware Rev               : 4.0
Num Ports                  : 128
Up Time                    : 19 min, 19 sec
Dell Networking OS Version : 9-4(0-168)
Jumbo Capable              : yes
POE Capable                : no
FIPS Mode                  : disabled
Burned In MAC              : 90:b1:1c:f4:9b:79
No Of MACs                 : 3

--  Power Supplies  --
Unit   Bay   Status     Type    FanStatus  FanSpeed(rpm)
--------------------------------------------------------------
  0     0    down       UNKNOWN down       0
  0     1    up         AC      up         6600

--  Fan  Status  --
Unit Bay  TrayStatus Fan0  Speed   Fan1  Speed
-----------------------------------------------------------------
0    0    up         up    7072    up    7021
0    1    up         up    7021    up    7123
0    2    up         up    7072    up    7021

Speed in RPM

--  Unit 1 --
Unit Type                  : Member Unit
Status                     : not present

--  Unit 2 --
Unit Type                  : Member Unit
Status                     : not present

--  Unit 3 --
Unit Type                  : Member Unit
Status                     : not present

--  Unit 4 --
Unit Type                  : Member Unit
Status                     : not present

--  Unit 5 --
Unit Type                  : Member Unit
Status                     : not present
```

Example (S4810)

```
Dell#show system stack-unit 0

--  Unit 0 --
Unit Type                  : Management Unit
Status                     : online
Next Boot                  : online
Required Type              : S6000 - 32-port TE/FG (SI)
Current Type               : S6000 - 32-port TE/FG (SI)
```

```
Master priority            : 0
Hardware Rev               : 4.0
Num Ports                  : 128
Up Time                    : 21 min, 8 sec
Dell Networking OS Version : 9-4(0-168)
Jumbo Capable              : yes
POE Capable                : no
FIPS Mode                  : disabled
Boot Flash                 : 3.1.1.2
Boot Selector              : 3.1.0.2
Memory Size                : 3203911680 bytes
Temperature                : 36C
Voltage                    : ok
Serial Number              : NA
Part Number                : 08YWFG     Rev A00
Vendor Id                  : DL
Date Code                  : 26092013
Country Code               : CN
Piece Part ID              : CN-08YWFG-28298-39Q-0015
PPID Revision              : A00
Service Tag                : 24N1VS1
Expr Svc Code              : 463 414 838 5
Auto Reboot                : disabled
Burned In MAC              : 90:b1:1c:f4:9b:79
No Of MACs                 : 3

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus   FanSpeed(rpm)
-------------------------------------------------------------
  0     0    down         UNKNOWN     down        0
  0     1    up           AC          up          6600

--  Fan  Status  --
Unit Bay   TrayStatus  Fan0    Speed   Fan1    Speed
-------------------------------------------------------------
0    0     up          up      6971    up      7021
0    1     up          up      7021    up      7021
0    2     up          up      7021    up      7021

Speed in RPM
```

Example (S6000–ON)

```
Dell>show system stack-unit 1

--  Unit 1 --
Unit Type                  : Management Unit
Status                      : Card Problem - Software Failure
Next Boot                  : online
Required Type              : S6000-ON - 32-port TE/FG (SI-ON)
Current Type               : S6000-ON - 32-port TE/FG (SI-ON)
Master priority            : 0
Hardware Rev               : 3.0
Num Ports                  : 128
Up Time                    : 3 day, 22 hr, 33 min
Dell Networking OS Version : 9-7(0-288)
Jumbo Capable              : yes
POE Capable                : no
FIPS Mode                  : disabled
Boot Flash                 : Present
Boot Selector              : 3.20.0.0
Memory Size                : 3203911680 bytes
Temperature                : 0C
Voltage                    : ok
Serial Number              : NA
Part Number                : <PART NUMB Rev R>
Vendor Id                  : NA
Date Code                  : NA
Country Code               : NA
Piece Part ID              : <SER:)0
```

```
PPID Revision              : R>
Service Tag                : N/A
Expr Svc Code              : 0
Auto Reboot                : disabled
Burned In MAC              : 00:00:00:00:00:00
No Of MACs                 : 3

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus   FanSpeed(rpm)
-------------------------------------------------------------
  1     1    up           AC      up          18528
  1     2    absent               absent      0

--  Fan  Status  --
Unit Bay   TrayStatus  Fan1    Speed   Fan2    Speed
-------------------------------------------------------------
 1    1     up          up      19275   up      19275
 1    2     absent
 1    3     up          up      19275   up      18904

Speed in RPM
```

telnet-peer-stack-unit

Connect through Telnet to a peer stack-unit from a port extender (PE) console.

C9000 Series

Syntax `telnet-peer-stack-unit`

Defaults Not configured.

Command Modes

- EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9 (0.0)	Introduced on the C9010 and C1048P.

Usage Information In a PE stack setup (master unit), use the `telnet-peer-stack-unit` command to open a telnet session to the port extender standby unit.

After connecting to the standby unit, you can access the following subset of commands:

```
Dell(standby)#?
cd                              Change current directory
copy                            Copy from one file to another
delete                          Delete a file
dir                             List files on a filesystem
disable                         Turn off privileged commands
enable                          Turn on privileged commands
exit                            Exit from the EXEC
format                          Format a filesystem
pwd                             Display current working directory
```

```
rename                          Rename a file
reset                           Reset selected card
show                            PE Show running system information
telnet-peer-stack-unit          Open a telnet connection to the peer stack-unit
```

Example

```
Dell#telnet-peer-stack-unit
Trying Unit 2...
Connected to Unit 2.
Exit character is '^]'.
Login: admin
Password:
Jun 24 10:14:11: %PE-UNKN-UNIT2-S:CP %SEC-5-LOGIN_SUCCESS: Login successful
for user admin on line vty0 ( Unit 3 )
Dell(standby)>en
Dell(standby)#exit
Session terminated for user admin on line vty 0 ( Unit 3 )

Closed connection.
Dell#Jun 24 10:14:29: %PE-UNKN-UNIT2-S:CP %SEC-5-LOGOUT: Exec session is
terminated for user admin on line vty0 ( Unit 3 )
```

upgrade system

Upgrade the Dell Networking OS image to the stack-unit.

C9000 Series

Syntax

```
upgrade system {stack-unit unit number | all } {usbflash: | flash:} {rpmA:|
rpmB:}
```

Parameters

stack-unit *unit number*	Enter the keyword `stack-unit` and specify the stack-unit ID to sync the image to that of the stack-unit or enter `all` to sync the image on all stack-units. The stack-unit number range is from 0 to 7.
all	Enter the keyword `all` to sync the image on all the stack-units configured.
flash: *file-url*	Enter the keyword `flash:` and specify the location of the image file in the format `//`*`directory-path`* or press Enter to launch a prompt sequence.
usbflash: *file-url*	Enter the keyword `usbflash:` and copy the image from usbflash file system`usbflash://`*`filepath`* press Enter to launch a prompt sequence.
rpmA: | rpm B:	Specify the flash partition of the operating-system image that you want to upgrade.

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.

Version	Description
9.7(0.0)	Added support for NFS mount.
9.2(1.0)	Introduced on the Z9500.
9.0(0.0)	Added support for IPv6 for the `file-url` parameter.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000. Added support for the SSD on the Z9000 only.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added support for TFTP and SCP.
7.6.1.0	Introduced on the S-Series.

Usage Information

You can specify the source location and can choose `usbflash:` or `flash:` as a source location. You can choose rmpA (for partition A) or rpm B (for partition B) as your destination. The system boots up from the newly upgraded partition after you reload the system with the `reload` command. To verify that the Dell Networking OS image was correctly upgraded, use thee `show boot system all` command.

For more information on the upgrade process, see the *Dell Networking C9010 and C1048P Release Notes*.

Example

```
Dell# upgrade system stack-unit 0 usbflash://FTOS-C1048.bin rpmA:
00:39:32 : Discarded 1 pkts. Expected block num : 51. Received block num: 50
!00:39:36 : Discarded 1 pkts. Expected block num : 65. Received block num: 64
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!..!
..........!!!!!!!!!!!!!!!!!!!!!
93924044 bytes successfully copied
System image upgrade completed successfully.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Image upgraded to all
```

41

PE Stacking

Use the commands in this chapter to configure and manage C1048P port-extender (PE) stacking. Stacking is not supported on C9010 switches.

For information about using the PE stacking feature, see the "Port Extender (PE) Stacking" chapter in the *Dell Networking OS Configuration Guide for the C9000 Series*.

You can use the commands to pre-configure a port extender, so that the configuration settings are invoked when the switch is attached to the chassis.

Topics:

- renumber
- reset
- show pe system
- show hardware pe
- stack unit
- stack-unit

renumber

To rearrange the stack units, reassign a stack unit ID number.

C9000 Series

Syntax `pe pe-id stack-unit unit number renumber unit number`

Parameters

pe *pe-id*	Enter the keyword `pe` and the PE ID. The range is from 0 to 255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the stack-unit ID number. The range is from 0 to 7.
renumber *unit number*	Enter the keyword `renumber` and a new stack-unit ID number. The range is from 0 to 7.

Default Default stack-unit number is zero.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command-Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Example

```
Dell# pe 255 stack-unit 0 renumber 2
```

reset

Reset or reboot the linecard, RPM, PE and PE stack-unit.

C9000 Series

Syntax

`reset {linecard slot-id | rpm slot id [hard] | pe pe-id [stack-unit unit-number]}`

From a **PE console**, use `reset stack-unit unit-number [hard]` to reset the stack-unit.

Parameters

linecard *slot-id*	Enter the keyword `linecard` and the *slot-id* number to specify the set of line-card ports for reset. The slot ID range is from 0 to 11.
rpm	Enter the keyword `rpm` and the *slot-id* number to specify the route processor module (RPM) ports for reset. The range for the RPM card ports is from 0 to 1.
hard	(Optional) Reboot (power cycle) the specified line card, RPM card, or PE stack-unit (The `hard` option for PE is only available from PE console).
pe *pe-id*	Enter the keyword `pe` and the port extender (PE) ID. The range for *pe-id* is from 0 to 255.
stack-unit *unit-number*	(Optional) Enter the keyword `stack-unit` and the stack-unit number. The range is from 0 to 7.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.3.1.0	Added the `hard reset` option.
7.8.1.0	Augmented to run on the standby unit in order to reset the standby unit directly.
7.7.1.0	Introduced on the S-Series.

Usage Information

Resetting is a soft reboot, including flushing the forwarding tables. The `hard` option is available for PE stack-unit from the PE console only.

To reset (soft reboot) a stack-unit from PE console, use the `reset` command and specify the stack-unit number. To perform a hard reset or power-cycle to a specified stack-unit, use the `reset stack-unit` *`unit-number`* `hard` command.

Example: linecard

```
Dell#reset linecard 0
Dell#Jun 24 15:26:39: %RPM1-P:CP %CHMGR-5-LINECARD_RESET: linecard 0 being
reset
Jun 24 15:26:39: %RPM1-P:CP %CHMGR-2-LINECARD_DOWN: linecard 0 down - reset
Jun 24 15:26:39: %RPM1-P:CP %IFMGR-1-DEL_PORT: Removed port: Fo 0/0-20,

Dell#Jun 24 15:28:24: %RPM1-P:CP %CHMGR-5-CHECKIN: Checkin from linecard 0
(type C9000LC0640, 24 ports)
Jun 24 15:28:24: %RPM1-P:CP %CHMGR-5-LINECARD_UP: linecard 0 is up
Jun 24 15:28:28: %C9000LC0640:0 %IFAGT-5-INSERT_OPTICS_QSFP: Optics QSFP
inserted in slot 0 port 0
Jun 24 15:28:28: %C9000LC0640:0 %IFAGT-5-INSERT_OPTICS_QSFP: Optics QSFP
inserted in slot 0 port 4
Jun 24 15:28:28: %C9000LC0640:0 %IFAGT-5-INSERT_OPTICS_QSFP: Optics QSFP
inserted in slot 0 port
16
```

Example: pe stack-unit

```
Dell#reset stack-unit 2
Dell#Jun 24 15:19:52: %PE255-UNIT1-M:CP %CHMGR-5-STACKUNIT_RESET: stack-unit 2
being reset
Jun 24 15:19:52: %PE255-UNIT1-M:CP %CHMGR-2-STACKUNIT_DOWN: stack-unit 2 down
- reset
Jun 24 15:19:53: %PE255-UNIT1-M:CP %IFMGR-5-OSTATE_DN: Changed interface state
to down: Te 2/48
Jun 24 15:19:53: %PE255-UNIT1-M:CP %IFMGR-1-DEL_PORT: Removed port: Te 2/48-49,
Jun 24 15:19:53: %PE255-UNIT2-S:CP %IFMGR-1-DEL_PORT: Removed port: Te 2/48-49,
Jun 24 15:19:58: %PE255-UNIT1-M:CP %POLLMGR-2-ALT_STACKUNIT_STATE: Alternate
Stack-unit is not present
Jun 24 15:19:58: %PE255-UNIT1-M:CP %CHMGR-2-STACKUNIT_DOWN: stack-unit 2 down
- card removed
Jun 24 15:20:06: %PE255-UNIT1-M:CP %POLLMGR-2-ALT_STACKUNIT_STATE: Alternate
Stack-unit is not present
Jun 24 15:20:06: %PE255-UNIT1-M:CP %POLLMGR-2-ALT_STACKUNIT_STATE: Alternate
Stack-unit is present
Jun 24 15:21:06: %PE-UNKN-UNIT3-S:CP %RAM-5-STACKUNIT_STATE: Stack-unit 3 is
in Standby State.
Jun 24 15:21:08: %PE255-UNIT3-S:CP %EVL-6-EVENT_LOGGING: Start uploading pre-
recorded traps(count:1) to CB
Jun 24 15:21:09: %PE255-UNIT3-S:CP %EVL-6-EVENT_LOGGING: Completed uploading
pre-recorded traps(send count:1, pending traps:0) to CB
Jun 24 15:21:21: %PE255-UNIT1-M:CP %CHMGR-5-STACKUNIT_DETECTED: stack-unit 2
present
Jun 24 15:21:23: %PE255-UNIT1-M:CP %CHMGR-5-CHECKIN: Checkin from stack-unit 2
(type C1048P, 52 ports)
Jun 24 15:21:23: %PE255-UNIT1-M:CP %CHMGR-5-STACKUNIT_UP: stack-unit 2 is up
Jun 24 15:21:25: %PE-UNKN-C1048P:2 %IFAGT-5-INSERT_OPTICS_PLUS: Optics SFP+
inserted in slot 2 port 48
Jun 24 15:21:26: %PE-UNKN-C1048P:2 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 60 % of the full speed
Jun 24 15:21:26: %PE255-UNIT1-M:CP %CHMGR-5-FANTRAY_INSERTED: Fan tray 0 of
Unit 2 is inserted
Jun 24 15:21:26: %PE255-UNIT1-M:CP %CHMGR-0-PS_UP: Power supply 0 in unit 2 is
up
Jun 24 15:21:26: %PE255-UNIT1-M:CP %CHMGR-0-PS_UP: Power supply 1 in unit 2 is
up
Jun 24 15:21:26: %PE-UNKN-C1048P:2 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 60 % of the full speed
Jun 24 15:21:26: %PE255-UNIT1-M:CP %IFMGR-5-OSTATE_UP: Changed interface state
```

```
to up: Te 2/48
Jun 24 15:21:27: %PE-UNKN-C1048P:2 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 75 % of the full speed
Jun 24 15:21:27: %PE255-UNIT1-M:CP %CHMGR-4-TEMP_STATUS_CHANGE:  Unit 2
temperature state changed to 1 (Current temperature 35C).
```

Related Commands

- reload – reboots the Dell Networking OS.

show pe system

Display information on all the system components of a port extender on a stack.

C9000 Series

Syntax

`show pe pe-id system [ brief | stack-port [status | topology] | stack-unit unit number ]`

Parameters

pe-id	Enter the port extender ID *pe-id* to view the port extender system status and details. Range is from 0 to 255.
brief	(Optional) Enter the keyword `brief` to view a short summary of the port extender system status.
stack-port	(Optional) Enter the keyword `stack port` to view the stack port information.
status	(Optional) Enter the keyword `status` to view the status of the stack ports when there is a PE stack configuration.
topology	(Optional) Enter the keyword `topology` to view the topology information when there is a PE stack configured. Topology for a PE stack can be: daisy chain or ring.
stack-unit *unit number*	(Optional) Enter the keyword `stack-unit` and a stack unit number to view information on a specified stack-unit in detail. Stack unit range is from 0 to 7.

Default

None

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

The `show pe pe-id system` output displays detailed summary on different hardware and software components of all the stack units attached to a port extender. You can use the `brief` option to view a short summary of the stack-units attached to a port extender. Use the `stack-port status` to view the status of the stack-units attached to a port extender. The `stack-port topology` option allows you to view whether the

stack is forming a daisy chain or a ring topology. Use the `stack-unit`*`unit—number`* option to display the detailed summary of both hardware and software components of a specific stack-unit.

Example: pe *pe-id* system

```
Dell#show pe 1 system

Stack MAC                  : 6c:c0:00:43:09:90

--  Unit 1 --
Unit Type                  : Management Unit
Status                     : online
Next Boot                  : online
Required Type              : C1048P - 48-port GE
Current Type               : C1048P - 48-port GE
Master priority            : 2
Hardware Rev               : 5.0
Num Ports                  : 52
Up Time                    : 22 hr, 40 min
Dell Networking OS Version : 1-0(0-4092)
Jumbo Capable              : yes
POE Capable                : yes
FIPS Mode                  : disabled
Burned In MAC              : 6c:c0:00:43:09:90
No Of MACs                 : 3

--  Power Supplies  --
Unit  Bay   Status   Type      FanStatus   FanSpeed(rpm)
----  ----  -------  --------  ----------  --------------
  1    0    up       AC         NA          NA
  1    1    absent              NA          NA

--  Fan  Status  --
Unit   Bay   TrayStatus  Fan0    Speed   Fan1    Speed
-----  ----  ----------  ------  ------  -----   --------
  1     0    up          up      9056    up      9056

Speed in RPM

Dell#
Dell#show pe 1 system brief

Stack MAC                  : 6c:c0:00:43:09:90

--  Stack Info  --
Unit  UnitType    Status        ReqTyp      CurTyp   Version    Ports
----  ----------  ------------  ----------  -------  ---------- -------
  0   Standby     not present
  1   Management  online        C1048P      C1048P   1-0(0-4092) 52
  2   Member      not present
  3   Member      not present
  4   Member      not present
  5   Member      not present
  6   Member      not present
  7   Member      not present

--  Power Supplies  --
Unit   Bay   Status       Type    FanStatus   FanSpeed(rpm)
----  -----  -----------  -------  ----------- ---------------------
  1     0    up           AC      NA          NA
  1     1    absent               NA          NA

--  Fan  Status  --
Unit   Bay   TrayStatus  Fan0    Speed   Fan1    Speed
----  -----  ----------  ------  ------  ------- ----------
  1     0     up          up      9056    up      9056

Speed in RPM
```

Example: brief

```
Dell>show pe 254 system brief

Stack MAC                  : 34:17:eb:00:a0:00

--  Stack Info  --
```

```
Unit  UnitType   Status       ReqTyp   CurTyp  Version    Ports
----- ---------- ----------- -------- -------  ----------  ------
  0   Unknown     online      C1048P   C1048P  1-0(0-4158) 52
  1   Unknown     not present
  2   Unknown     not present
  3   Unknown     not present
  4   Unknown     not present
  5   Unknown     not present
  6   Unknown     not present
  7   Unknown     not present
```

Example: stack port status

```
Dell#show pe 0 system stack-ports status
Topology: Ring
Interface  Link Speed       Admin     Link
             (Gb/s)         Status    Status
-----------------------------------------------
  0/1          24            up        up
  0/2          24            up        up
  1/1          24            up        up
  1/2          24            up        up
  2/1          24            up        up
  2/2          24            up        up
  3/1          24            up        up
  3/2          24            up        up
  4/1          24            up        up
  4/2          24            up        up
  5/1          24            up        up
  5/2          24            up        up
  6/1          24            up        up
  6/2          24            up        up
  7/1          24            up        up
  7/2          24            up        up
```

Example: stack port topology

```
Dell#show pe 253 system stack-ports topology
Topology: Ring
Interface  Connection
---------  -----------
  0/1       2/51
  0/2       1/50
  1/50      0/51
  1/51      2/50
  2/50      1/51
  2/51      0/50
```

Example: stack-unit *unit-number*

```
Dell#show pe 1 system stack-unit 1

--  Unit 1 --
Unit Type                  : Management Unit
Status                     : online
Next Boot                  : online
Required Type              : C1048P - 48-port GE
Current Type               : C1048P - 48-port GE
Master priority            : 2
Hardware Rev               : 5.0
Num Ports                  : 52
Up Time                    : 22 hr, 42 min
Dell Networking OS Version : 1-0(0-4092)
Jumbo Capable              : yes
POE Capable                : yes
FIPS Mode                  : disabled
Boot Flash                 : 3.3.1.7
Boot Selector              : Present
Memory Size                : 1073741824 bytes
Temperature                : 32C
Voltage                    : ok
Serial Number              : NA
Part Number                : 7590009701 Rev 001
```

```
Vendor Id                   : NA
Date Code                   : NA
Country Code                : NA
Piece Part ID               : US-0F14T0-77951-3AG-000A
PPID Revision               : 01
Service Tag                 : NA
Expr Svc Code               : NA
Auto Reboot                 : enabled
Burned In MAC               : 6c:c0:00:43:09:90
No Of MACs                  : 128

--  Power Supplies  --
Unit   Bay   Status     Type       FanStatus    FanSpeed(rpm)
----- ----- ---------- --------  -----------  -------------
  1     0    up         AC         NA           NA
  1     1    absent                NA           NA

--  Fan  Status  --
Unit   Bay   TrayStatus  Fan0    Speed   Fan1    Speed
----- ------ ---------- ------- ------- -------- -----------------
  1     0     up          up      9056    up      9056

Speed in RPM
```

show hardware pe

Display input and output traffic statistics and other operational information about a specified hardware component.

C9000 Series

Syntax

```
show hardware pe pe-id stack-unit unit number {cpu | drops | stack-port | unit}
```

Parameters

pe *pe-id* stack unit *unit-number*

Enter `pe pe-id stack-unit unit number` parameters with a command option to display hardware statistics from the specified port extender (PE) and stack-unit. The port extender ID range is from 0 to 255 and the stack-unit ID range is from 0 to 7. The command options are:

- `cpu data-plane statistics`: Displays data-plane statistics, including the`bc pci` driver statistics for the device.
- `drops unit unit number [user—port {port {port-num | range}]`: Displays the number of internal drops of control-plane and protocol control packets on the port specified. User port range is 1–51.
- `stack-port` Displays traffic statistics for the stacking ports on a specified PE.
- `unit` *unit-number* to view with the following options:
  - `counters`: Displays the traffic counters.
  - `details`: Displays more detailed hardware information.
  - `port-stats`: Displays the internal statistics on a per-port basis.
  - `register`: Displays the internal registers.
  - `table-dump`: Displays the tables from the bShell.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.2(0.0)	Modified the `drops` keyword range, unit keyword `range` and added the `buffer` and `cpu management statistics` options.
8.3.19.0	Introduced on the S4820T.
8.3.11.5	Added i2c statistics and sata-interfaces statistics.
8.3.11.4	Added user port information.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Modified the `stack-port` keyword range expanded from 49-52 to 0-52; output modified for the `cpu data-plane statistics` option; the following options were added: `drops [unit 0-1 [port 0-27]]` and `unit 0-1 {counters | details | port-stats [detail] | register}`
7.7.1.0	Introduced on the S-Series.

Example (Port Extender Statistics)

```
Dell>show hardware pe 0 stack-unit 0 cpu data-plane statistics

bc pci driver statistics for device:
 rxHandle        :15451
 noMhdr          :0
 noMbuf          :0
 noClus          :0
 recvd           :15451
 dropped         :0
 recvToNet       :15451
 rxError         :0
 rxFwdError      :0
 rxDatapathErr   :0
 rxPkt(COS0 )    :0
 rxPkt(COS1 )    :0
 rxPkt(COS2 )    :0
 rxPkt(COS3 )    :0
 rxPkt(COS4 )    :0
 rxPkt(COS5 )    :0
 rxPkt(COS6 )    :9304
 rxPkt(COS7 )    :3
 rxPkt(COS8 )    :6144
 rxPkt(COS9 )    :0
 rxPkt(COS10)   :0
 rxPkt(COS11)   :0
 rxPkt(UNIT0)    :15451
 transmitted     :15250
 txRequested     :15250
 noTxDesc        :0
 txError         :0
```

```
txReqTooLarge    :0
txInternalError :0
txDatapathErr    :0
txPkt(COS0 )     :0
txPkt(COS1 )     :0
txPkt(COS2 )     :0
txPkt(COS3 )     :0
txPkt(COS4 )     :0
txPkt(COS5 )     :0
txPkt(COS6 )     :0
txPkt(COS7 )     :0
txPkt(COS8 )     :0
txPkt(COS9 )     :0
txPkt(COS10)    :0
txPkt(COS11)    :0
txPkt(UNIT0)     :0
```

Example (PE Stack-Port: Drops)

```
Dell>show hardware pe 0 stack-unit 0 drops user-port 1
Dell#sho hardware pe 255 stack-unit 3 drops user-port 47
Drops in Interface PeGi 255/3/47:
--- Ingress Drops      ---
Ingress Drops                  : 13049
IBP CBP Full Drops             : 0
PortSTPnotFwd Drops            : 13049
IPv4 L3 Discards               : 0
Policy Discards                : 0
Packets dropped by FP          : 0
(L2+L3) Drops                  : 0
Port bitmap zero Drops         : 13049
Rx VLAN Drops                  : 0
--- Ingress MAC counters---
Ingress FCSDrops               : 0
Ingress MTUExceeds             : 0
--- MMU Drops          ---
Ingress MMU Drops              : 0
HOL DROPS(TOTAL)               : 1208454
HOL DROPS on COS0              : 0
HOL DROPS on COS1              : 0
HOL DROPS on COS2              : 0
HOL DROPS on COS3              : 0
HOL DROPS on COS4              : 0
HOL DROPS on COS5              : 0
```

Related Commands

clear hardware system-flow — clears the statistics from selected hardware components.

show system — displays the current status of all the stack members or a specific member.

stack unit

Pre-provision the specified port-extender stack unit.

C9000 Series

Syntax

`stack-unit` *unit-number* {`type` *unit-type* | `priority` *value*}

To de-provision or delete a port extender stack unit, use the `no stack-unit` *unit-number* {`type` *unit-type* | `priority` *value*} command.

Parameters

stack-unit *unit-number*	Enter the stack-unit ID number to locate a specific stack unit. Stack unit number range is 0–7.
type *PE-type*	Enter a value for the stack-unit type.
priority *value*	Enter the master priority value for the unit. The priority value range is from 1 to 14. The unit with the numerically highest priority value is elected the master.

Default None

Command Modes PE CONFIG

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command-Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Introduced the port extender types for the N20xx and N30xx series.
9.9(0.0)	Introduced on the C9010.

Usage Information You can pre-provision a port extender stack unit using the `stack unit` command in the PE configuration mode and specify the stack-unit type. Only similar types of stack units are provisioned under a single port extender. The maximum number of stack units allowed for provisioning is 8. In a PE stack, by default, the stack unit with the highest MAC address is elected master; the stack unit with the second highest MAC address is elected standby. To change the default master and standby assignment, you can assign stack-unit`priority value`. If multiple units tie for the highest priority, the unit with the highest MAC address is elected master.

In the following example, **stack-unit 0** with priority 14 is the master and **stack-unit 1** with priority 13 is the standby.

NOTE: You can configure a stack-unit priority only when the unit is online.

Example (stack-unit priority)

```
Dell(conf)#pe 2
Dell(conf-pe-2)#stack-unit 0 priority 14
Dell(conf-pe-2)#stack-unit 1 priority 13
```

Example (stack unit type)

```
Dell(conf-pe-201)#stack-unit 1 type ?
C1048P                  52-port GE/TE
N2024-PE                28-port GE/TE
N2024P-PE               28-port GE/TE
N2048-PE                52-port GE/TE
N2048P-PE               52-port GE/TE
N3024-PE                28-port GE/TE
N3024F-PE               28-port GE/TE
N3024P-PE               28-port GE/TE
N3048-PE                52-port GE/TE
N3048P-PE               52-port GE/TE
Dell(conf-pe-201)#
```

Example (stack unit type)

```
Dell(conf-pe-5)#stack-unit 4 type C1048P
```

```
Dell(conf-pe-5)# show config
!
pe provision 5
 stack-unit 4 type C1048P
```

Related Commands

- redundancy force-failover — Force the standby unit to become the primary or master unit

- reset — Reset or reboot the linecard, RPM, PE and PE stack-unit.

stack-unit

Extend the unused uplink ports as access ports.

Syntax

`stack-unit` *`unit-id`* `access—ports` *`port-range`*

To convert the port back to uplink, use the `no stack-unit` *`unit-id`* `access—ports` *`port-range`* command.

Parameters

stack-unit *unit-id*	Enter the keyword `stack-unit` and the stack unit-id number. The stack-unit range is from 0 to 7.
access-ports *port-range*	Enter the keyword `access-ports` and the port-range, separated by comma. There are maximum of 4 uplink ports in a PE, and the range is from 1 to 4.

NOTE: Enter the *`port-range`* as 1 to 2 for front–end uplink ports and 3 to 4 for uplink ports in back panel (available in N30xx).

Default

None

Command Modes

PE CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command-Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced support for extending unused uplink port as access-port.

Usage Information

You can configure the unused uplink port as access-port even on a provisioned PE.

Example

```
DellEMC(conf)# pe provision 2
DellEMC(conf-pe-2)# stack-unit 1 access-ports 1
DellEMC(conf-pe-2)#
```

Example (stack unit type)

```
Dell(conf-pe-2)# show config
!
pe provision 2
 stack-unit 1 type C1048P
 stack-unit 1 access-ports 1
 stack-unit 3 type N2024P-PE
 cascade interface TenGigabitEthernet 1/2
```

42

Per-VLAN Spanning Tree Plus (PVST+)

The Dell Networking operating software implementation of per-VLAN spanning tree plus (PVST+) is based on the IEEE 802.1w standard spanning tree protocol.

NOTE: For easier command line entry, the plus (+) sign is not used at the command line.

Topics:

- description
- disable
- extend system-id
- protocol spanning-tree pvst
- show spanning-tree pvst
- spanning-tree pvst
- spanning-tree pvst err-disable
- tc-flush-standard
- vlan bridge-priority
- vlan forward-delay
- vlan hello-time
- vlan max-age

description

Enter a description of the PVST+.

C9000 Series

Syntax

`description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the spanning tree (80 characters maximum).

Defaults

none

Command Modes

SPANNING TREE PVST+ (The prompt is “config-pvst”.)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.1	Introduced.

Related Commands protocol spanning-tree pvst — enter SPANNING TREE mode on the switch.

disable

Disable PVST+ globally.

C9000 Series

Syntax `disable`

To enable PVST+, use the `no disable` command.

Defaults Disabled.

Command Modes CONFIGURATION (conf-pvst)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands protocol spanning-tree pvst — enter PVST+ mode.

extend system-id

To augment the Bridge ID with a VLAN ID so that PVST+ differentiate between BPDUs for each VLAN, use extend system ID. If the VLAN receives a BPDU meant for another VLAN, PVST+ does not detect a loop, and both ports can remain in Forwarding state.

C9000 Series

Syntax `extend system-id`

Defaults Disabled

Command Modes PROTOCOL PVST

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced.

Example

```
Dell(conf-pvst)#do show spanning-tree pvst vlan 5 brief
VLAN 5
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32773, Address 0001.e832.73f7
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32773 (priority 32768 sys-id-ext 5), Address 0001.e832.73f7
We are the root of Vlan 5
Configured hello time 2, max age 20, forward delay 15

Interface Designated
Name    PortID  Prio  Cost  Sts Cost Bridge ID      PortID
-----------------------------------------------------------
Te 0/10 128.140 128  200000 FWD 0   32773 0001.e832.73f7 128.140
Te 0/12 128.142 128  200000 DIS 0   32773 0001.e832.73f7 128.142

Interface
Name     Role PortID  Prio  Cost  Sts Cost Link-type Edge
-------------------------------------------------------
Te 0/10  Desg 128.140 128  200000 FWD 0    P2P       No
Te 0/12  Dis  128.142 128  200000 DIS 0    P2P       No
```

Related Commands protocol spanning-tree pvst – enter SPANNING TREE mode on the switch.

protocol spanning-tree pvst

To enable PVST+ on a device, enter the PVST+ mode.

C9000 Series

Syntax

```
protocol spanning-tree pvst
```

To disable PVST+, use the `disable` command.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
8.3.1.0	Introduced.

Example

```
Dell#conf
Dell(conf)#protocol spanning-tree pvst
Dell(conf-pvst)#no disable
Dell(conf-pvst)#vlan 2 bridge-priority 4096
Dell(conf-pvst)#vlan 3 bridge-priority 16384
Dell(conf-pvst)#
Dell(conf-pvst)#show config
!
protocol spanning-tree pvst
  no disable
  vlan 2 bridge-priority 4096
  vlan 3 bridge-priority 16384
Dell#
```

Usage Information

After you enable PVST+, the device runs an STP instance for each VLAN it supports.

Related Commands

disable — disables PVST+.

show spanning-tree pvst — displays the PVST+ configuration.

show spanning-tree pvst

View the Per-VLAN spanning tree configuration.

C9000 Series

Syntax `show spanning-tree pvst [vlan vlan-id] [brief] [guard] [interface interface]`

Parameters

vlan *vlan-id* (OPTIONAL) Enter the keyword `vlan` then the VLAN ID. The range is 1 to 4094.

brief (OPTIONAL) Enter the keyword `brief` to view a synopsis of the PVST+ configuration information.

interface *interface* (OPTIONAL) Enter one of the interface keywords along with the slot/port information:

- For a Port Channel interface, enter the keyword `port-channel` then a number: The range is 1 to 4096.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

guard (OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on a PVST interface and the current port state.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.4.2.1	Support for the optional `guard` keyword was added on the C-Series, S-Series, and E-Series TeraScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Expanded to display port error disable state (EDS) caused by loopback BPDU inconsistency and Port VLAN ID inconsistency.
6.2.1.1	Introduced.

Usage Information

The following describes the `show spanning-tree pvst` command shown in the following examples.

Field	Description
Interface Name	PVST interface.
Instance	PVST instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

The `peGigE` ports and VP-LAG ports information is displayed as part of the`show spanning-tree 0` command output, only when the `guard` option is entered.

Example (Brief)

```
Dell#show spanning-tree pvst vlan 3 brief
VLAN 3
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 4096, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15

Interface                              Designated
Name    PortID  Prio Cost Sts Cost   Bridge ID      PortID
-----------------------------------------------------------
Te 1/0  128.130 128 20000 FWD 20000 4096 0001.e801.6aa8  128.426
Te 1/1  128.131 128 20000 BLK 20000 4096 0001.e801.6aa8  128.427
Te 1/16 128.146 128 20000 FWD 20000 16384 0001.e805.e306 128.146
Te 1/17 128.147 128 20000 FWD 20000 16384 0001.e805.e306 128.147

Interface
Name    Role PortID   Prio Cost  Sts Cost Link-type Edge
-------------------------------------------------------
Te 1/0  Root 128.130  128  20000 FWD 20000 P2P      No
Te 1/1  Altr 128.131  128  20000 BLK 20000 P2P      No
Te 1/16 Desg 128.146  128  20000 FWD 20000 P2P      Yes
Te 1/17 Desg 128.147  128  20000 FWD 20000 P2P      Yes
```

Example

```
Dell#show spanning-tree pvst vlan 2
VLAN 2
Root Identifier has priority 4096, Address 0001.e805.e306
Root Bridge hello time 2, max age 20, forward delay 15
Bridge Identifier has priority 4096, Address 0001.e805.e306
Configured hello time 2, max age 20, forward delay 15
We are the root of VLAN 2
Current root has priority 4096, Address 0001.e805.e306
```

```
Number of topology changes 3, last change occured 00:57:00

Port 130 (TenGigabitEthernet 1/0) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.130
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.130, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 3
The port is not in the Edge port mode

Port 131 (TenGigabitEthernet 1/1) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.131
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.131, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1567, received 0
The port is not in the Edge port mode

Port 146 (TenGigabitEthernet 1/16) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.146
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.146, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1578, received 0
The port is in the Edge port mode

Port 147 (TenGigabitEthernet 1/17) is designated Forwarding
Port path cost 20000, Port priority 128, Port Identifier 128.147
Designated root has priority 4096, address 0001.e805.e3:06
Designated bridge has priority 4096, address 0001.e805.e3:06
Designated port id is 128.147, designated path cost 0
Number of transitions to forwarding state 1
BPDU sent 1579, received 0
The port is in the Edge port mode
```

Example (EDS/LBK)

```
Dell#show spanning-tree pvst vlan 2 interface tengigabitethernet 1/0

TenGigabitEthernet 1/0 of VLAN 2 is LBK_INC discarding

Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 152, received 27562

Interface Designated
Name    PortID   Prio Cost  Sts Cost Bridge ID       PortID
-------------------------------------------------------------
Te 1/0  128.1223 128  20000 EDS 0 32768 0001.e800.a12b 128.1223
```

Example (EDS/PVID)

```
Dell#show spanning-tree pvst vlan 2 interface tengigabitethernet 1/0

TenGigabitEthernet 1/0 of VLAN 2 is PVID_INC discarding

Edge port:no (default) port guard :none (default)
Link type: point-to-point (auto) bpdu filter:disable (default)
Bpdu guard :disable (default)
Bpdus sent 1, received 0

Interface Designated
Name   PortID   Prio Cost  Sts Cost Bridge ID       PortID
-------------------------------------------------------------
Te 1/0 128.1223 128 20000 EDS 0 32768 0001.e800.a12b 128.1223
```

Example (Guard)

```
Dell#show spanning-tree pvst vlan 5 guard
Interface
Name   Instance Sts         Guard type
---------------------------------
Te 0/1 5        INCON(Root) Rootguard
Te 0/2 5        FWD         Loopguard
Te 0/3 5        EDS(Shut)   Bpduguard
```

Related Commands spanning-tree pvst — configure PVST+ on an interface.

spanning-tree pvst

Configure a PVST+ interface with one of these settings: edge port with optional bridge port data unit (BPDU) guard, port disablement if an error condition occurs, port priority or cost for a VLAN range, loop guard, or root guard.

C9000 Series

Syntax

```
spanning-tree pvst {edge-port [bpduguard [shutdown-on-violation]] | err-disable
| vlan vlan-range {cost number | priority value} | loopguard | rootguard}
```

Parameters

edge-port	Enter the keywords `edge-port` to configure the interface as a PVST+ edge port.
bpduguard	Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.
shutdown-on-violation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.
err-disable	Enter the keywords `err-disable` to enable the port to be put into the error-disable state (EDS) if an error condition occurs.
vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
cost *number*	Enter the keyword `cost` then the port cost value. The range is from 1 to 200000. Defaults: • 10-Gigabit Ethernet interface = **2000**. • Port Channel interface with one 10 Gigabit Ethernet = **2000**. • Port Channel with two 10 Gigabit Ethernet = **1800**.
priority *value*	Enter the keyword `priority` then the Port priority value in increments of 16. The range is from 0 to 240. The default is **128**.
loopguard	Enter the keyword `loopguard` to enable loop guard on a PVST+ port or port-channel interface.
rootguard	Enter the keyword `rootguard` to enable root guard on a PVST+ port or port-channel interface.

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Introduced the `loopguard` and `rootguard` options on the E-Series TeraScale, C-Series, and S-Series.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced the hardware `shutdown-on-violation` option.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the optional Bridge Port Data Unit (BPDU) guard.
6.2.1.1	Introduced.

Usage Information The BPDU guard option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into the Error Disable state if a BPDU appears, and a message is logged so that the administrator can take corrective action.

NOTE: A port configured as an edge port, on a PVST switch, immediately transitions to the forwarding state. Only ports connected to end-hosts should be configured as an edge port. Consider an edge port similar to a port with a spanning-tree portfast enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the route process module (RPM) CPU.

You cannot enable `root guard` and `loop guard` at the same time on a port. For example, if you configure `loop guard` on a port on which `root guard` is already configured, the following error message is displayed: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

When used in a PVST+ network, loop guard is performed per-port or per-port channel at a VLAN level. If no BPDUs are received on a VLAN interface, the port or port-channel transitions to a Loop-Inconsistent (blocking) state only for this VLAN.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

On PE ports and on VP-LAGs (LAGs formed with PE ports)

- Spanning-tree with `bpdu guard shutdown-on-violation` is enabled by default

- No spanning tree command is valid. This command is not visible and issuing this command on VP-LAG ports results in a failure.

-

Example

```
Dell(conf-if-te-1/1)#spanning-tree pvst vlan 3 cost 18000
Dell(conf-if-te-1/1)#end
Dell(conf-if-te-1/1)#show config
!
interface TenGigabitEthernet 1/1
  no ip address
  switchport
  spanning-tree pvst vlan 3 cost 18000
  no shutdown
Dell(conf-if-te-1/1)#end
```

Related Commands

show spanning-tree pvst — views the PVST+ configuration.

spanning-tree pvst err-disable

Place ports in an Err-Disabled state if they receive a PVST+ BPDU when they are members an untagged VLAN.

C9000 Series

Syntax

```
spanning-tree pvst err-disable cause invalid-pvst-bpdu
```

Defaults

Enabled; ports are placed in the Err-Disabled state if they receive a PVST+ BPDU when they are members of an untagged VLAN.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced.

Usage Information

Some non-Dell Networking systems which have hybrid ports participating in PVST+ transmit two kinds of BPDUs: an 802.1D BPDU and an untagged PVST+ BPDU.

Dell Networking systems do not expect PVST+ BPDU on an untagged port. If this happens, the system places the port in the Error-Disable state. This behavior might result in the network not converging. To prevent the system

from executing this action, use the `no spanning-tree pvst err-disable` command cause `invalid-pvst-bpdu`.

Related Commands show spanning-tree pvst — views the PVST+ configuration.

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

C9000 Series

Syntax `tc-flush-standard`

To disable, use the `no tc-flush-standard` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Usage Information By default, the system implements an optimized flush mechanism for PVST+. This implementation helps in flushing the MAC addresses only when necessary (and less often) allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn this *knob* command on to enable flushing MAC addresses after receiving every topology change notification.

vlan bridge-priority

Set the PVST+ bridge-priority for a VLAN or a set of VLANs.

C9000 Series

Syntax

`vlan vlan-range bridge-priority value`

To return to the default value, use the `no vlan bridge-priority` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
bridge-priority *value*	Enter the keywords `bridge-priority` then the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is **32768**.

Defaults

32768

Command Modes

CONFIGURATION (conf-pvst)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced.

Related Commands

vlan forward-delay — changes the time interval before the system transitions to the Forwarding state.

vlan hello-time — change the time interval between BPDUs.

vlan max-age — changes the time interval before PVST+ refreshes.

show spanning-tree pvst — displays the PVST+ configuration.

vlan forward-delay

Set the amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

C9000 Series

Syntax

`vlan vlan-range forward-delay seconds`

To return to the default setting, use the `no vlan forward-delay` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
forward-delay *seconds*	Enter the keywords `forward-delay` then the time interval, in seconds, that the system waits before transitioning PVST+ to the forwarding state. The range is from 4 to 30 seconds. The default is **15 seconds**.

Defaults

15 seconds

Command Modes

CONFIGURATION (conf-pvst)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced.

Related Commands

vlan bridge-priority — sets the bridge-priority value.

vlan hello-time — changes the time interval between BPDUs.

vlan max-age — changes the time interval before PVST+ refreshes.

show spanning-tree pvst — displays the PVST+ configuration.

vlan hello-time

Set the time interval between generation of PVST+ 7 BPDUs.

C9000 Series

Syntax

`vlan vlan-range hello-time seconds`

To return to the default value, use the `no vlan hello-time` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
hello-time *seconds*	Enter the keywords `hello-time` then the time interval, in seconds, between transmission of BPDUs. The range is from 1 to 10 seconds. The default is **2 seconds**.

Defaults

2 seconds

Command Modes

CONFIGURATION (conf-pvst)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced.

Related Commands

- vlan bridge-priority — sets the bridge-priority value.
- vlan forward-delay — changes the time interval before Dell Networking OS transitions to the forwarding state.
- vlan max-age — changes the time interval before PVST+ refreshes.
- show spanning-tree pvst — displays the PVST+ configuration.

vlan max-age

To maintain configuration information before refreshing that information, set the time interval for the PVST+ bridge.

C9000 Series

Syntax

`vlan vlan-range max-age seconds`

To return to the default, use the `no vlan max-age` command.

Parameters

vlan *vlan-range*	Enter the keyword `vlan` then the VLAN numbers. The range is from 1 to 4094.
max-age *seconds*	Enter the keywords `max-age` then the time interval, in seconds, that the system waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is **20 seconds**.

Defaults

20 seconds

Command Modes

CONFIGURATION (conf-pvst)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced.

Related Commands

vlan bridge-priority — sets the bridge-priority value.

vlan forward-delay — changes the time interval before the system transitions to the forwarding state.

vlan hello-time — changes the time interval between BPDUs.

show spanning-tree pvst — displays the PVST+ configuration.

43

PIM-Source Specific Mode (PIM-SSM)

The protocol-independent multicast source-specific mode (PIM-SSM) commands in this section are supported in the Dell Networking operating system.

Topics:

- IPv4 PIM Commands
- IPv4 PIM-Source Specific Mode Commands

IPv4 PIM Commands

The following commands apply to IPv4 PIM-SM, IPv4 PIM-SSM, and PIM-DM.

- clear ip pim tib
- debug ip pim
- ip pim dr-priority
- ip pim neighbor-filter
- ip pim query-interval
- show ip pim interface
- show ip pim neighbor
- show ip pim tib

clear ip pim tib

Clear PIM tree information from the PIM database.

C9000 Series

Syntax `clear ip pim tib [group]`

Parameters

group	(OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.

Version	Description
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information

If you use this command on a local VLT node, all multicast routes from the local PIM TIB, the entire multicast route table, and all the entries in the data plane are deleted. The local VLT node sends a request to the peer VLT node to download multicast routes learned by the peer. Both local and synced routes are removed from the local VLT node multicast route table. The peer VLT node clears synced routes from the node.

If you use this command on a peer VLT node, only the synced routes are deleted from the multicast route table.

debug ip pim

View IP PIM debugging messages.

C9000 Series

Syntax

```
debug ip pim [bsr | events | group | packet [in | out] | register | state |
timer [assert | hello | joinprune | register]]
```

To disable PIM debugging, use the `no debug ip pim` command or use the `undebug all`to disable all debugging command.

Parameters

bsr	(OPTIONAL) Enter the keyword `bsr` to view PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword `group` to view PIM messages for a specific group.
group	(OPTIONAL) Enter the keyword `group` to view PIM messages for a specific group.
packet [in | out]	(OPTIONAL) Enter the keyword `packet` to view PIM packets. Enter one of the optional parameters: • `in`: to view incoming packets • `out`: to view outgoing packets
register	(OPTIONAL) Enter the keyword `register` to view PIM register address in dotted decimal format (A.B.C.D).
state	(OPTIONAL) Enter the keyword `state` to view PIM state changes.
timer [assert | hello | joinprune | register]	(OPTIONAL) Enter the keyword `timer` to view PIM timers. Enter one of the optional parameters: • `assert`: to view the assertion timer • `hello`: to view the PIM neighbor keepalive timer • `joinprune`: to view the expiry timer (join/prune timer)

- `register`: to view the register suppression timer

Defaults Disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

ip pim dr-priority

Change the designated router (DR) priority for the interface.

C9000 Series

Syntax `ip pim dr-priority priority-value`

To remove the DR priority value assigned, use the `no ip pim dr-priority` command.

Parameters

priority-value	Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is 1.

Defaults 1

Command Modes INTERFACE

INTERFACE (BATCH Mode)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series on port-channels and the S-Series.

Usage Information The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.

ip pim neighbor-filter

To prevent a router from participating in protocol independent multicast (PIM), configure this feature.

C9000 Series

Syntax `ip pim neighbor-filter {access-list}`

To remove the restriction, use the `no ip pim neighbor-filter {access-list}` command.

Parameters

access-list	Enter the name of a standard access list. Maximum 16 characters.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information Do not enter this command before creating the access-list.

ip pim query-interval

Change the frequency of PIM Router-Query messages.

C9000 Series

Syntax `ip pim query-interval seconds`

To return to the default value, use the `no ip pim query-interval seconds` command.

Parameters

seconds	Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is **30 seconds**.

Defaults **30 seconds**

Command Modes INTERFACE

INTERFACE (BATCH Mode)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.

Version	Description
7.8.1.0	Introduced on the C-Series for the port-channels and the S-Series.

show ip pim interface

View information on the interfaces with IP PIM enabled.

C9000 Series

Syntax

```
show ip pim interface
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information

The following describes the `show ip pim interface` command shown in the following example.

Field	Description
Address	Lists the IP addresses of the interfaces participating in PIM.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.
Ver/Mode	Displays the PIM version number and mode for each interface participating in PIM: • v2 = PIM version 2 • S = PIM Sparse mode
Nbr Count	Displays the number of PIM neighbors discovered over this interface.
Query Intvl	Displays the query interval for Router Query messages on that interface (configured with `ip pim query-interval` command).

Field	Description
DR Prio	Displays the Designated Router priority value configured on the interface (use the `ip pim dr-priority` command).
DR	Displays the IP address of the Designated Router for that interface.

The `show ip pim interface` command does not display information corresponding to the loop-back interfaces.

Example

```
Dell#show ip pim interface
Address         Interface Ver/ Nbr   Query DR   DR
                          Mode Count Intvl Prio
172.21.200.254 Te 0/9     v2/S 0     30 1  172.21.200.254
172.60.1.2     Te 0/11    v2/S 0     30 1  172.60.1.2
192.3.1.1      Te 0/16    v2/S 1     30 1  192.3.1.1
192.4.1.1      Te 1/5     v2/S 0     30 1  192.4.1.1
172.21.110.1   Te 1/6     v2/S 0     30 1  172.21.110.1
172.21.203.1   Te 1/7     v2/S 0     30 1  172.21.203.1
```

show ip pim neighbor

View PIM neighbors.

C9000 Series

Syntax `show ip pim neighbor`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information The following describes the `show ip pim neighbor` command shown in the following example.

Field	Description
Neighbor address	Displays the IP address of the PIM neighbor.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.
Uptime/expires	Displays the amount of time the neighbor has been up then the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
Ver	Displays the PIM version number. • v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode. • 1 = default Designated Router priority (use the `ip pim dr-priority` command) • DR = Designated Router • S = Sparse mode

Example

```
Dell#show ip pim neighbor↵
Neighbor Interface Uptime/Expires Ver DR↵
Address Prio/Mode↵
127.87.3.4 Te 1/16 09:44:58/00:01:24 v2 1 / S↵
```

show ip pim tib

View the PIM tree information base (TIB).

C9000 Series

Syntax `show ip pim tib [group-address [source-address]]`

Parameters

group-address	(OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D).
source-address	(OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information The following describes the `show ip pim tib` command shown in the following example.

Field	Description
(S, G)	Displays the entry in the multicast PIM database.
uptime	Displays the amount of time the entry has been in the PIM route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.
flags	List the flags to define the entries: • D = PIM Dense Mode • S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = Dell Networking OS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K = acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/ source.
RPF neighbor	Displays the next hop from this interface towards the RP/source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: • a directly connect member of the Group • statically configured member of the Group • received a (*,G) Join message

Example

```
Dell#do show ip pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned,
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT,
       M - MSDP created entry, A - Candidate for MSDP Advertisement
       K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 00:40:16, expires 00:00:00, RP 20.40.4.4, flags: SCJ
  Incoming interface: Vlan 2007, RPF neighbor 20.30.124.4
  Outgoing interface list:
```

```
    Vlan 2006  Forward/Sparse   00:06:21/Never

(20.10.4.9, 225.1.1.1), uptime 00:06:21, expires 00:02:06, flags: CT
  Incoming interface: Vlan 2007, RPF neighbor 20.30.124.4
  Outgoing interface list:
    Vlan 2006  Forward/Sparse   00:06:21/Never

(*, 225.1.1.2), uptime 00:40:15, expires 00:00:00, RP 20.40.4.4, flags: SCJ
  Incoming interface: Vlan 2007, RPF neighbor 20.30.124.4
  Outgoing interface list:
    Vlan 2006  Forward/Sparse   00:06:21/Never

(20.10.4.9, 225.1.1.2), uptime 00:06:21, expires 00:02:06, flags: CT
  Incoming interface: Vlan 2007, RPF neighbor 20.30.124.4
  Outgoing interface list:
    Vlan 2006  Forward/Sparse   00:06:21/Never
```

IPv4 PIM-Source Specific Mode Commands

The following IPv4 PIM-source specific mode (PIM-SSM) commands are supported:

- ip pim ssm-range
- show ip pim ssm-range

ip pim ssm-range

Specify the SSM group range using an access list.

C9000 Series

Syntax `ip pim ssm-range {access_list_name}`

Parameters

access_list_name	Enter the name of the access list.

Defaults Default SSM range is 232/8 and ff3x/32

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON
9.7(0.0)	Introduced on the S6000-ON. Added support for VRF on S6000, S4810, S4820T, Z9000, Z9500, and S6000–ON.
9.7(0.0)	Added support for VRF.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

Usage Information

Dell Networking OS supports standard access lists for the SSM range. You cannot use extended ACLs for configuring the SSM range. If you configure an extended ACL and then used in the `ip pim ssm-range {access list name}` configuration, an error is reported.

However, if you configure `ip pim ssm-range {access list name}` first and then you configure the ACL as an Extended ACL, an error is not reported and the ACL is not applied to the SSM range.

Dell Networking OS-recommended best-practices are to configure the standard ACL, and then apply the ACL to the SSM range. After the SSM range is applied, the changes are applied internally without requiring clearing of the tree information base (TIB).

When the ACL rules change, the ACL and protocol-independent multicast (PIM) modules apply the new rules automatically.

When you configure the SSM range, Dell Networking OS supports SSM for configured group range as well as the default SSM range.

When you remove the SSM ACL, PIM SSM is supported for the default SSM range only.

show ip pim ssm-range

Display the non-default groups added using the SSM range feature.

C9000 Series

Syntax

```
show ip pim ssm-range
```

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added support for VRF on S6000, S4810, S4820T, Z9000, Z9500, and S6000–ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

Example

```
Group Address    / MaskLen
```

44

PIM-Sparse Mode (PIM-SM)

The protocol-independent multicast sparse-mode (PIM-SM) commands in this section are supported in the Dell Networking operating system.

Topics:

- IPv4 PIM-Sparse Mode Commands
- IPv6 PIM-Sparse Mode Commands

IPv4 PIM-Sparse Mode Commands

The following describes the IPv4 PIM-sparse mode (PIM-SM) commands.

clear ip pim rp-mapping

The bootstrap router (BSR) feature uses this command to remove all or particular rendezvous point (RP) advertisement.

C9000 Series

Syntax `clear ip pim rp-mapping [rp-address]`

Parameters

rp-address	(OPTIONAL) Enter the RP address in dotted decimal format (A.B.C.D).

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information This command re-applies the RP mapping logic for all the groups learnt by the node. Any stale information corresponding to the existing mapping configuration is updated. As a result, the existing BSR cache and the *,G's are deleted only if these entries are stale.

clear ip pim tib

Clear PIM tree information from the PIM database.

C9000 Series

Syntax `clear ip pim tib [group]`

Parameters

group	(OPTIONAL) Enter the multicast group address in dotted decimal format (A.B.C.D).

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information If you use this command on a local VLT node, all multicast routes from the local PIM TIB, the entire multicast route table, and all the entries in the data plane are deleted. The local VLT node sends a request to the peer VLT node to download multicast routes learned by the peer. Both local and synced routes are removed from the local VLT node multicast route table. The peer VLT node clears synced routes from the node.

If you use this command on a peer VLT node, only the synced routes are deleted from the multicast route table.

debug ip pim

View IP PIM debugging messages.

C9000 Series

Syntax

```
debug ip pim [bsr | events | group | packet [in | out] | register | state |
timer [assert | hello | joinprune | register]]
```

To disable PIM debugging, use the `no debug ip pim` command or use the `undebug all`to disable all debugging command.

Parameters

bsr	(OPTIONAL) Enter the keyword `bsr` to view PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword `group` to view PIM messages for a specific group.
group	(OPTIONAL) Enter the keyword `group` to view PIM messages for a specific group.
packet [in | out]	(OPTIONAL) Enter the keyword `packet` to view PIM packets. Enter one of the optional parameters: • `in`: to view incoming packets • `out`: to view outgoing packets
register	(OPTIONAL) Enter the keyword `register` to view PIM register address in dotted decimal format (A.B.C.D).
state	(OPTIONAL) Enter the keyword `state` to view PIM state changes.
timer [assert | hello | joinprune | register]	(OPTIONAL) Enter the keyword `timer` to view PIM timers. Enter one of the optional parameters: • `assert`: to view the assertion timer • `hello`: to view the PIM neighbor keepalive timer • `joinprune`: to view the expiry timer (join/prune timer) • `register`: to view the register suppression timer

Defaults

Disabled.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

ip pim bsr-border

Define the border of PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

C9000 Series

Syntax

```
ip pim bsr-border
```

To return to the default value, use the `no ip pim bsr-border` command.

Defaults

Disabled.

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information

This command is applied to the subsequent PIM-BSR. Existing BSR advertisements are cleaned up by time-out. To clean the candidate RP advertisements, use the `clear ip pim rp-mapping` command.

ip pim bsr-candidate

To join the Bootstrap election process, configure the PIM router.

C9000 Series

Syntax

`ip pim bsr-candidate` *`interface`* `][`*`hash-mask-length`*`] [`*`priority`*`]`

To return to the default value, use the `no ip pim bsr-candidate` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
hash-mask-length	(OPTIONAL) Enter the hash mask length. The range is from zero (0) to 32. The default is **30**.
priority	(OPTIONAL) Enter the priority used in Bootstrap election process. The range is from zero (0) to 255. The default is **zero (0)**.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.1.1.0	Introduced on the E-Series ExaScale.
6.1.1.0	Added support for the VLAN interface.

ip pim dr-priority

Change the designated router (DR) priority for the interface.

C9000 Series

Syntax

`ip pim dr-priority` *priority-value*

To remove the DR priority value assigned, use the `no ip pim dr-priority` command.

Parameters

priority-value	Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is 1.

Defaults

1

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series on port-channels and the S-Series.

Usage Information

The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.

ip pim graceful-restart

This feature permits configuration of non-stop forwarding (NSF or graceful restart) capability on a PIM enabled router.

Syntax `ip pim graceful-restart {nsf [restart-time | stale-entry-time]}`

Parameters

nsf	Enter the keyword `nsf` to configure the non-stop forwarding capability. **NOTE: `ip pim graceful-restart nsf` is applicable for the entire multicast sub-system.**
restart-time	(OPTIONAL) Enter the keywords `restart-time` followed by the number of seconds estimated for the PIM speaker to restart. The range is 30 to 300 seconds. The default is **180 seconds**.
stale-entry-time	(OPTIONAL) Enter the keywords `stale-entry-time` followed by the number of seconds for which entries are kept alive after restart. The range is 30 to 300 seconds. The default is **60 seconds**.

Defaults as above

Command Modes CONFIGURATION

Command History

Version	Description
9.14(0.0)	Added support on the C9000.
9.0(1.3)	Introduced on the S5000.
8.2.1.0	Introduced on the E-Series ExaScale. Added the `ipv6` option for the E-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information The PIM-SM component uses the graceful-restart feature to relearn the PIM JOIN messages (*,G/S,G) from upstream neighbors. The upstream neighbors detect the RPM failover of the downstream router, on reception of a different gen-id in the PIM-hello message. They then start to send relevant PIM JOINs to the downstream router after establishing neighbor-ship with the new active RPM.

ip pim join-filter

Permit or deny PIM Join/Prune messages on an interface using an extended IP access list. This command prevents the PIM-SM router from creating state based on multicast source and/or group.

C9000 Series

Syntax `ip pim [vrf vrf-name] join-filter ext-access-list`

To remove the access list, use the `no ip pim [vrf vrf-name] join-filter ext-access-list` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to permit or deny PIM join or prune messages on an interface associated with that VRF.
ext-access-list	Enter the name of an extended access list.

Defaults none

Command Modes INTERFACE

INTERFACE (BATCH Mode)

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Removed the in and out parameters. Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series for the port-channels and the S-Series.
7.7.1.0	Introduced on the E-Series.

Example

```
Dell(conf)# ip access-list extended iptv-channels
Dell(config-ext-nacl)# permit ip 10.1.2.3/24 225.1.1.0/24
Dell(config-ext-nacl)# permit ip any 232.1.1.0/24
Dell(config-ext-nacl)# permit ip 100.1.1.0/16 any
Dell(config-if-te-1/1)# ip pim join-filter iptv-channels
Dell(config-if-te-1/1)# ip pim join-filter iptv-channels
```

Related Commands ip access-list extended — configure an access list based on IP addresses or protocols.

ip pim ingress-interface-map

When the Dell Networking system is the RP, statically map potential incoming interfaces to (*,G) entries to create a lossless multicast forwarding environment.

C9000 Series

Syntax `ip pim ingress-interface-map std-access-list`

Parameters

std-access-list	Enter the name of a standard access list.

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.1.0	Introduced

Example

```
Dell(conf)# ip access-list standard map1
Dell(config-std-nacl)# permit 224.0.0.1/24
Dell(config-std-nacl)#exit
Dell(conf)#int tengig 1/1
Dell(config-if-te-1/1)# ip pim ingress-interface-map map1
```

ip pim neighbor-filter

To prevent a router from participating in protocol independent multicast (PIM), configure this feature.

C9000 Series

Syntax `ip pim neighbor-filter {access-list}`

To remove the restriction, use the `no ip pim neighbor-filter {access-list}` command.

Parameters

access-list	Enter the name of a standard access list. Maximum 16 characters.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series and S-Series.
7.6.1.0	Introduced on the E-Series.

Usage Information Do not enter this command before creating the access-list.

ip pim query-interval

Change the frequency of PIM Router-Query messages.

C9000 Series

Syntax `ip pim query-interval seconds`

To return to the default value, use the `no ip pim query-interval seconds` command.

Parameters

seconds	Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is **30 seconds**.

Defaults **30 seconds**

Command Modes INTERFACE

INTERFACE (BATCH Mode)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series for the port-channels and the S-Series.

ip pim register-filter

To prevent a PIM source DR from sending register packets to an RP for the specified multicast source and group, use this feature.

C9000 Series

Syntax

`ip pim register-filter` *`access-list`*

To return to the default, use the `no ip pim register-filter access-list [vrf` *`vrf-name`*`]` command.

Parameters

access-list	Enter the name of an extended access list. Maximum 16 characters.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added support for VRF.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.
7.6.1.0	Introduced

Usage Information

The access name is an extended IP access list that denies PIM register packets to RP at the source DR based on the multicast and group addresses. Do not enter this command before creating the access-list

.

ip pim rp-address

Configure a static PIM rendezvous point (RP) address for a group or access-list.

C9000 Series

Syntax

`ip pim rp-address` *`address`* `{group-address` *`group-address mask`*`} [override]`

To remove an RP address, use the `no ip pim rp-address` *`address`* `{group-address` *`group-address mask`*`} [vrf` *`vrf-name`*`] [override]` command.

Parameters

address	Enter the RP address in dotted decimal format (A.B.C.D).
group-address *group-address mask*	Enter the keywords `group-address` then a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.
override	Enter the keyword `override` to override the BSR updates with static RP. The override takes effect immediately during enable/disable. **NOTE: This option is applicable to multicast group range.**

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.
pre- 6.1.1.1	Introduced on the E-Series.

Usage Information First-hop routers use this address by to send register packets on behalf of source multicast hosts. The RP addresses are stored in the order in which they are entered. RP addresses learned using BSR take priority over static RP addresses. Without the `override` option, RPs advertised by the BSR updates take precedence over the statically configured RPs.

ip pim rp-candidate

To send out a Candidate-RP-Advertisement message to the bootstrap (BS) router or define group prefixes that are defined with the RP address to PIM BSR, configure a PIM router.

C9000 Series

Syntax `ip pim rp-candidate {interface [priority] [acl-name]}`

To return to the default value, use the `no ip pim rp-candidate {interface [priority]}[vrf vrf-name]` command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

priority (OPTIONAL) Enter the priority used in Bootstrap election process. The range is zero (0) to 255. The default is **192**.

acl-name (OPTIONAL) Enter the name of an ACL to configure a PIM router to act as an RP for a specific set of multicast group addresses that are defined in the ACL.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.0.0	Introduced the `acl-name` parameter.
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.
pre- 6.1.1.1	Introduced on the E-Series.

Usage Information

Priority is stored at BSR router when receiving a Candidate-RP-Advertisement.

ip pim sparse-mode

Enable PIM sparse mode and IGMP on the interface.

C9000 Series

Syntax

```
ip pim sparse-mode
```

To disable PIM sparse mode and IGMP, use the `no ip pim sparse-mode` command.

Defaults

Disabled.

Command Modes

INTERFACE

INTERFACE (BATCH Mode)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.

Version	Description
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series for the port-channels and the S-Series.

Usage Information The interface must be enabled (the `no shutdown` command) and not have the `switchport` command configured. Multicast must also be enabled globally (using the `ip multicast-lag-hashing` command). PIM is supported on the port-channel interface.

ip pim spt-threshold

To switch to the shortest path tree when the traffic reaches the specified threshold value, configure the PIM router.

C9000 Series

Syntax `ip pim spt-threshold [infinity]`

To return to the default value, use the `no ip pim spt-threshold [infinity] [vrf vrf-name]` command.

Parameters

infinity	(OPTIONAL) Enter the keyword `infinity` to never switch to the source-tree.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added support for VRF.
9.5(0.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.

Usage Information This command is applicable to last hop routers on the shared tree towards the rendezvous point (RP).

ip pim sparse-mode sg-expiry-timer

Enable expiry timers globally for all sources.

C9000 Series

Syntax

`ip pim sparse-mode sg-expiry-timer` *seconds*

To disable configured timers and return to default mode, use the `no ip pim sparse-mode sg-expiry-timer` command.

Parameters

seconds	Enter the number of seconds the S, G entries are retained. The range is from 211 to 65535.

Defaults

Disabled. The default expiry timer (with no times configured) is 210 sec.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON and added support for VRF.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the C-Series for the port-channels and the S-Series.
7.7.1.1	Introduced

Usage Information

This command configures an expiration timer for all S.G entries, unless they are assigned to an Extended ACL.

Even though the FHR nodes act as RPs, these nodes still send *Register encap* messages to themselves and expect to receive a *Register stop* message (for Anycast RP support). As a result, if the DLT timer expires, SG is not deleted until the register state is deleted in the node. This register state expires 210 seconds after the last Null register is received.

show ip pim bsr-router

View information on the Bootstrap router.

C9000 Series

Syntax `show ip pim bsr-router`

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Example

```
Dell#show ip pim bsr-router
PIMv2 Bootstrap information
This system is the Bootstrap Router (v2)
  BSR address: 7.7.7.7 (?)
  BSR Priority: 0, Hash mask length: 30
  Next bootstrap message in 00:00:08

This system is a candidate BSR
  Candidate BSR address: 7.7.7.7, priority: 0, hash mask length: 30
```

show ip pim snooping neighbor

Display information on PIM neighbors learned through PIM-SM snooping.

C9000 Series

Syntax

```
show ip pim snooping neighbor [vlan vlan-id]
```

Parameters

vlan *vlan-id*	(OPTIONAL) Enter a VLAN ID to display information about PIM neighbors that PIM-SM snooping discovered on a specified VLAN. The valid VLAN IDs range is from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.1.1	Introduced on the E-Series ExaScale.

Usage Information

The following describes the `show ip pim snooping neighbor` commands shown in the following example.

Field	Description
Neighbor address	Displays the IP address of the neighbor learned through PIM-SM snooping.
Interface	Displays the VLAN ID number and slot/port on which the PIM-SM-enabled neighbor was discovered.
Uptime/expires	Displays the amount of time the neighbor has been up then the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
Ver	Displays the PIM version number: • v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode: • 1 = default Designated Router priority (use the `ip pim dr-priority` command) • DR = Designated Router • S = Sparse mode

Example

```
Dell#show ip pim snooping neighbor

Neighbor    Interface          Uptime/Expires    Ver  DR Prio
Address
165.87.32.2   Vl 2 [Te 1/13 ]  00:04:03/00:01:42  v2  1
165.87.32.10  Vl 2 [Te 1/11 ]  00:00:46/00:01:29  v2  0
165.87.32.12  Vl 2 [Te 41/20 ] 00:00:51/00:01:24  v2  0
```

show ip pim interface

View information on the interfaces with IP PIM enabled.

C9000 Series

Syntax `show ip pim interface`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information The following describes the `show ip pim interface` command shown in the following example.

Field	Description
Address	Lists the IP addresses of the interfaces participating in PIM.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), of the interfaces participating in PIM.
Ver/Mode	Displays the PIM version number and mode for each interface participating in PIM: • v2 = PIM version 2 • S = PIM Sparse mode
Nbr Count	Displays the number of PIM neighbors discovered over this interface.

Field	Description
Query Intvl	Displays the query interval for Router Query messages on that interface (configured with `ip pim query-interval` command).
DR Prio	Displays the Designated Router priority value configured on the interface (use the `ip pim dr-priority` command).
DR	Displays the IP address of the Designated Router for that interface.

The `show ip pim interface` command does not display information corresponding to the loop-back interfaces.

Example

```
Dell#show ip pim interface
Address         Interface Ver/ Nbr   Query DR   DR
                          Mode Count Intvl Prio
172.21.200.254 Te 0/9     v2/S 0     30 1  172.21.200.254
172.60.1.2     Te 0/11    v2/S 0     30 1  172.60.1.2
192.3.1.1      Te 0/16    v2/S 1     30 1  192.3.1.1
192.4.1.1      Te 1/5     v2/S 0     30 1  192.4.1.1
172.21.110.1   Te 1/6     v2/S 0     30 1  172.21.110.1
172.21.203.1   Te 1/7     v2/S 0     30 1  172.21.203.1
```

show ip pim neighbor

View PIM neighbors.

C9000 Series

Syntax `show ip pim neighbor`

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information The following describes the `show ip pim neighbor` command shown in the following example.

Field	Description
Neighbor address	Displays the IP address of the PIM neighbor.
Interface	List the interface type, with either slot/port information or ID (VLAN or Port Channel), on which the PIM neighbor was found.
Uptime/expires	Displays the amount of time the neighbor has been up then the amount of time until the neighbor is removed from the multicast routing table (that is, until the neighbor hold time expires).
Ver	Displays the PIM version number. • v2 = PIM version 2
DR prio/Mode	Displays the Designated Router priority and the mode. • 1 = default Designated Router priority (use the `ip pim dr-priority` command) • DR = Designated Router • S = Sparse mode

Example

```
Dell#show ip pim neighbor↵
Neighbor Interface Uptime/Expires Ver DR↵
Address Prio/Mode↵
127.87.3.4 Te 1/16 09:44:58/00:01:24 v2 1 / S↵
```

show ip pim rp

View all multicast groups-to-RP mappings.

C9000 Series

Syntax `show ip pim rp [mapping | group-address]`

Parameters

mapping	(OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learnt.
group-address	(OPTIONAL) Enter the multicast group address mask in dotted decimal format to view RP for a specific group.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Example

```
Dell#show ip pim rp
Group           RP
224.2.197.115   165.87.20.4
224.2.217.146   165.87.20.4
224.3.3.3       165.87.20.4
225.1.2.1       165.87.20.4
225.1.2.2       165.87.20.4
229.1.2.1       165.87.20.4
229.1.2.2       165.87.20.4
Dell#
```

Example (Mapping)

```
Dell#show ip pim rp mapping
PIM Group-to-RP Mappings
Group(s): 224.0.0.0/4, Static
  RP: 50.40.4.4, v2
Dell#
```

Example (Address)

```
Dell#show ip pim rp 229.1.2.1
Group          RP
229.1.2.1    165.87.20.4
```

show ip pim snooping interface

Display information on VLAN interfaces with PIM-SM snooping enabled.

C9000 Series

Syntax `show ip pim snooping interface [vlan vlan-id]`

Parameters

vlan *vlan-id*	(OPTIONAL) Enter a VLAN ID to display information about a specified VLAN configured for PIM-SM snooping. The valid VLAN IDs range is from 1 to 4094.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.1.1	Introduced on the E-Series ExaScale.

Usage Information

The following describes the `show ip pim snooping interface` commands shown in the following example.

Field	Description
Interface	Displays the VLAN interfaces with PIM-SM snooping enabled.
Ver/Mode	Displays the PIM version number for each VLAN interface with PIM-SM snooping enabled: • v2 = PIM version 2 • S = PIM Sparse mode
Nbr Count	Displays the number of neighbors learned through PIM-SM snooping on the interface.
DR Prio	Displays the Designated Router priority value configured on the interface (`ip pim dr-priority` command).
DR	Displays the IP address of the Designated Router for that interface.

Example (#2)

```
Dell#show ip pim snooping interface
Interface Ver Nbr    DR    DR
              Count  Prio
Vlan 2    v2  3      1     165.87.32.2
```

show ip pim summary

View information about PIM-SM operation.

C9000 Series

Syntax `show ip pim summary [vrf vrf-name]`

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword vrf followed by the name of the VRF to configure this setting on that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added support for VRF.
9.5(0.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.1	Support for the display of PIM-SM snooping status was added on E-Series ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Example

```
Dell# show ip pim summary

PIM TIB version 495
Uptime 22:44:52
Entries in PIM-TIB/MFC : 2/2

Active Modes :
        PIM-SNOOPING

Interface summary:
        1 active PIM interface
        0 passive PIM interfaces
        3 active PIM neighbors

TIB summary:
       1/1 (*,G) entries in PIM-TIB/MFC
       1/1 (S,G) entries in PIM-TIB/MFC
       0/0 (S,G,Rpt) entries in PIM-TIB/MFC

       0 PIM nexthops
       0 RPs
       0 sources
       0 Register states

Message summary:
       2582/2583 Joins sent/received
       5/0 Prunes sent/received
       0/0 Candidate-RP advertisements sent/received
       0/0 BSR messages sent/received
       0/0 State-Refresh messages sent/received
       0/0 MSDP updates sent/received
       0/0 Null Register messages sent/received
       0/0 Register-stop messages sent/received

Data path event summary:
```

```
      0 no-cache messages received
      0 last-hop switchover messages received
      0/0 pim-assert messages sent/received
      0/0 register messages sent/received
```

show ip pim tib

View the PIM tree information base (TIB).

C9000 Series

Syntax `show ip pim tib [group-address [source-address]]`

Parameters

group-address	(OPTIONAL) Enter the group address in dotted decimal format (A.B.C.D).
source-address	(OPTIONAL) Enter the source address in dotted decimal format (A.B.C.D).

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Introduced on the S-Series.

Usage Information

The following describes the `show ip pim tib` command shown in the following example.

Field	Description
(S, G)	Displays the entry in the multicast PIM database.
uptime	Displays the amount of time the entry has been in the PIM route table.
expires	Displays the amount of time until the entry expires and is removed from the database.
RP	Displays the IP address of the RP/source for this entry.
flags	List the flags to define the entries: • D = PIM Dense Mode

Field	Description
	• S = PIM Sparse Mode • C = directly connected • L = local to the multicast group • P = route was pruned • R = the forwarding entry is pointing toward the RP • F = Dell Networking OS is registering this entry for a multicast source • T = packets were received via Shortest Tree Path • J = first packet from the last hop router is received and the entry is ready to switch to SPT • K = acknowledge pending state
Incoming interface	Displays the reverse path forwarding (RPF) interface towards the RP/ source.
RPF neighbor	Displays the next hop from this interface towards the RP/source.
Outgoing interface list:	Lists the interfaces that meet one of the following criteria: • a directly connect member of the Group • statically configured member of the Group • received a (*,G) Join message

Example

```
Dell#do show ip pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned,
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT,
       M - MSDP created entry, A - Candidate for MSDP Advertisement
       K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(*, 225.1.1.1), uptime 00:40:16, expires 00:00:00, RP 20.40.4.4, flags: SCJ
  Incoming interface: Vlan 2007, RPF neighbor 20.30.124.4
  Outgoing interface list:
    Vlan 2006  Forward/Sparse   00:06:21/Never

(20.10.4.9, 225.1.1.1), uptime 00:06:21, expires 00:02:06, flags: CT
  Incoming interface: Vlan 2007, RPF neighbor 20.30.124.4
  Outgoing interface list:
    Vlan 2006  Forward/Sparse   00:06:21/Never

(*, 225.1.1.2), uptime 00:40:15, expires 00:00:00, RP 20.40.4.4, flags: SCJ
  Incoming interface: Vlan 2007, RPF neighbor 20.30.124.4
  Outgoing interface list:
    Vlan 2006  Forward/Sparse   00:06:21/Never

(20.10.4.9, 225.1.1.2), uptime 00:06:21, expires 00:02:06, flags: CT
  Incoming interface: Vlan 2007, RPF neighbor 20.30.124.4
  Outgoing interface list:
    Vlan 2006  Forward/Sparse   00:06:21/Never
```

show running-config pim

Display the current configuration of PIM-SM snooping.

C9000 Series

Syntax `show running-config pim`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Introduced on the E-Series ExaScale.

Example

```
Dell#show running-config pim
!
ip pim snooping enable
```

IPv6 PIM-Sparse Mode Commands

The following describes the IPv6 PIM-sparse mode (PIM-SM) commands.

clear ipv6 pim tib

Clear the IPv6 PIM multicast-routing database (tree information base—TIB).

Syntax `clear ipv6 pim [vrf vrf-name] tib [group-address]`

Parameters

vrf *vrf-name* (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF.

NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

group-address (OPTIONAL) Enter the multicast group address in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zero.

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Related Commands show ipv6 pim tib – displays the IPv6 PIM tree information base (TIB)

debug ipv6 pim

Invoke IPv6 PIM debugging.

Syntax `debug ipv6 pim [vrf vrf-name] [bsr | events | group [group] | packet [in | out] | register [group] | state | timer [assert | hello | joinprune | register]]`

To disable IPv6 PIM debugging, use the `no debug ipv6 pim [vrf vrf-name]` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view IP PIM debugging messages corresponding to that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**
bsr	(OPTIONAL) Enter the keyword `bsr` to invoke debugging of IPv6 PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword `events` to invoke debugging of IPv6 PIM events.
group [*group*]	(OPTIONAL) Enter the keyword `group` followed by the group address to invoke debugging on that specific group.
packet	(OPTIONAL) Enter the keyword `packet` to invoke debugging of IPv6 PIM packets.
register [*group*]	(OPTIONAL) Enter the keyword `register` and optionally the group address to invoke debugging of IPv6 PIM register messages for a particular group.
state	(OPTIONAL) Enter the keyword `state` to view IPv6 PIM state changes.
timer [assert | hello | joinprune | register]	(OPTIONAL) Enter the keyword `timer` to view IPv6 PIM timers. Enter one of the optional parameters: • `assert`: to view the assertion timer • `hello`: to view the IPv6 PIM neighbor keepalive timer • `joinprune`: to view the expiry timer (join/prune timer) • `register`: to view the register suppression timer

Defaults Disabled.

Command Modes EXEC Privilege

Command History

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

ipv6 pim bsr-border

Define the border of IPv6 PIM domain by filtering inbound and outbound PIM-BSR messages per interface.

Syntax `ipv6 pim bsr-border`

To return to the default value, use the `no ipv6 pim bsr-border` command.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

9.14(1.0)	Introduced on the C9010, S3048–ON, S3100 Series, S4048–ON, S4048T–ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON.

Usage Information This command is applied to the subsequent PIM-BSR. Existing BSR advertisements are cleaned up by time-out.

ipv6 pim bsr-candidate

To join the Bootstrap election process, configure the PIM router as a bsr-candidate.

Syntax `ipv6 pim [vrf vrf-name] bsr-candidate interface [hash-mask-length] [priority]`

To return to the default value, use the `no ipv6 pim bsr-candidate [vrf vrf-name]` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` then the name of the VRF to configure the PIM router on a VRF.
interface	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383. • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
hash-mask-length	(OPTIONAL) Enter the hash mask length. The range is from eight (8) to 128. The default is **126**.
priority	(OPTIONAL) Enter the priority used in Bootstrap election process. The range is from zero (0) to 255. In the BSR election process, the BSR with the higher priority takes the

precedence. If the priority values are equal, the router with the higher IP address becomes the BSR. The default is **0**.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.0)	Introduced on the C9010, S3048-ON, S3100 Series, S4048-ON, S4048T-ON, S6000-ON, S6010-ON, S6100-ON, Z9100-ON.

ipv6 pim dr-priority

Change the designated router (DR) priority for the IPv6 interface.

Syntax `ipv6 pim dr-priority` *priority-value*

To remove the DR priority value assigned, use the `no ipv6 pim dr-priority` command.

Parameters

priority-value	Enter a number. Preference is given to larger/higher number. The range is from 0 to 4294967294. The default is **1**.

Defaults **1**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Usage Information The router with the largest value assigned to an interface becomes the designated router. If two interfaces contain the same designated router priority value, the interface with the largest interface IP address becomes the designated router.

ipv6 pim query-interval

Change the frequency of IPv6 PIM router-query messages.

Syntax `ipv6 pim query-interval` *seconds*

To return to the default value, use the `no ipv6 pim query-interval` *seconds* command.

Parameters

seconds — Enter a number as the number of seconds between router query messages. The range is from 0 to 65535. The default is **30 seconds**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

ipv6 pim rp-address

Configure a static PIM rendezvous point (RP) address for a group. First-hop routers use this address to send register packets on behalf of the source multicast host.

Syntax `ipv6 pim [vrf vrf-name] rp-address address {group-address group-address mask} [override]`

To remove an RP address, use the `no ipv6 pim re-address address group-address mask [override]` command.

Parameters

vrf *vrf-name* — (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view IP PIM debugging messages corresponding to that VRF.

NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

address — Enter the IPv6 RP address in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zero.

group-address *group-address mask* — Enter the keywords `group-address` then the group address in the x:x:x:x::x format and then the mask in /nn format to assign that group address to the RP.

NOTE: The :: notation specifies successive hexadecimal fields of zero.

override — (OPTIONAL) Enter the keyword `override` to override the BSR updates with static RP. The override takes effect immediately during enable/disable.

NOTE: This option is applicable to multicast group range.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Usage Information

The device selects the RP based on the longest prefix match of the configured group address when both static and dynamic RPs are configured.

The `override` option allow you to use statically configured RP instead of the longest prefix match of the configured group address associated with a dynamic RP.

ipv6 pim rp-candidate

Configure an IPv6 PIM router to send out a Candidate-RP-Advertisement message to the bootstrap (BS) router or define group prefixes that are defined with the RP address to PIM BSR.

Syntax

`ipv6 pim [vrf vrf-name] rp-candidate {interface [priority] [acl-name]}`

To return to the default value, use the `no ipv6 pim [vrf vrf-name] rp-candidate {interface [priority]}` command.

Parameters

vrf *vrf-name*

(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF.

NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

interface

Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For a port-channel interface, enter the keywords `port-channel` then the port-channel ID.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

priority

(OPTIONAL) Enter the priority used in RP election process. The range is zero (0) to 255. The default is **192**. In the RP election process, the RP with the lower priority takes the precedence.

acl-name

(OPTIONAL) Enter the name of an ACL to configure a PIM router to act as an RP for a specific set of multicast group addresses that are defined in the ACL.

NOTE: If you do not specify the `acl-name`, the system uses the default multicast IPv6 group range, which is ff00::/8.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.0)	Introduced on the C9010, S3048–ON, S3100 Series, S4048–ON, S4048T–ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON.

Usage Information

Priority is stored at BSR router when receiving a Candidate-RP-Advertisement.

ipv6 pim sparse-mode

Enable IPv6 PIM sparse mode and MLD on the interface.

Syntax

`ipv6 pim sparse-mode`

To disable IPv6 PIM sparse mode and MLD on the interface, use the `no ipv6 pim sparse-mode` command.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Usage Information

Enable the interface (use the `no shutdown` command) and not have the `switchport` command configured. Also enable Multicast globally. PIM is supported on the port-channel interface.

ipv6 pim sparse-mode sg-expiry-timer

Enable expiry timers globally for all sources.

Syntax

`ipv6 pim [vrf vrf-name] sparse-mode sg-expiry-timer seconds`

To disable configured timers and return to default mode, use the `no ipv6 pim sparse-mode sg-expiry-timer` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword vrf followed by the name of the VRF to enable expiry timer for all sources on that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**
seconds	Enter the number of seconds the S, G entries are retained. The range is from 211 to 65535.

Defaults

Disabled. The default expiry timer (with no times configured) is 210 sec.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Usage Information This command configures an expiration timer for all S.G entries, unless they are assigned to an Extended ACL.

Even though the FHR nodes act as RPs, these nodes still send *Register encap* messages to themselves and expect to receive a *Register stop* message (for Anycast RP support). As a result, if the DLT timer expires, SG is not deleted until the register state is deleted in the node. This register state expires 210 seconds after the last Null register is received.

ipv6 pim spt-threshold

Specifies when a PIM leaf router should join the shortest path tree.

Syntax `ipv6 pim [vrf vrf-name] spt-threshold {infinity}`

To return to the default value, use the `no ipv6 pim spt-threshold` command.

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view IP PIM debugging messages corresponding to that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**
infinity	Enter the keyword `infinity` to have all sources for the specified group use the shared tree and never join shortest path tree (SPT).

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Usage Information PIM leaf routers join the shortest path tree immediately after the first packet arrives from a new source.

show ipv6 pim bsr-router

View information on the bootstrap router.

Syntax

```
show ipv6 pim [vrf vrf-name] bsr-router
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.0)	Introduced on the C9010, S3048–ON, S3100 Series, S4048–ON, S4048T–ON, S6000–ON, S6010–ON, S6100–ON, Z9100–ON.

Example

```
DellEMC#show ipv6 pim bsr-router
PIMv2 Bootstrap information
  BSR address: 200::1 (?)
  BSR Priority: 0, Hash mask length: 126
  Expires:     00:01:43

This system is a candidate BSR
  Candidate BSR address: 100::1, priority: 0, hash mask length: 126

Next Cand_RP_advertisement in 00:00:25
  RP: 100::1(Lo 0)
DellEMC#
```

show ipv6 pim interface

Display IPv6 PIM enabled interfaces.

Syntax

```
show ipv6 pim [vrf vrf-name] interface
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view IP PIM debugging messages corresponding to that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Example

```
DellEMC#show ipv6 pim interface
Interface     Ver/     Nbr      Query    DR
              Mode     Count    Intvl    Prio
Te 1/1        v2/S     1        30       101
Address : fe80::4e76:25ff:fee5:32c2
DR      : this router

Te 1/2        v2/S     1        30       100
Address : fe80::4e76:25ff:fee5:32c2
DR      : this router

Te 1/3        v2/S     0        30       1
Address : fe80::4e76:25ff:fee5:32c2
DR      : this router
```

show ipv6 pim neighbor

Displays IPv6 PIM neighbor information.

Syntax `show ipv6 pim [vrf vrf-name] neighbor [detail]`

]Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view IP PIM debugging messages corresponding to that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**
detail	(OPTIONAL) Enter the keyword `detail` to displayed PIM neighbor detailed information.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Example

```
DellEMC#show ipv6 pim neighbor
Neighbor                  Interface Uptime/Expires     Ver  DR
Address                                                    Prio/Mode
fe80::201:e8ff:fe02:140f  Te 1/11   01:44:59/00:01:16  v2   1 / S
fe80::201:e8ff:fe00:6265  Te 1/12   01:45:00/00:01:16  v2   1 / DR
DellEMC#
```

show ipv6 pim rp

View all IPv6 multicast groups-to-rendezvous point (RP) mappings.

Syntax

```
show ipv6 pim [vrf vrf-name] rp [mapping | group-address]
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view IP PIM debugging messages corresponding to that VRF.
mapping	(OPTIONAL) Enter the keyword `mapping` to display the multicast groups-to-RP mapping and information on how RP is learned.
group-address	(OPTIONAL) Enter the multicast group address in the x:x:x:x::x format to view RP mappings for a specific group. **NOTE: The :: notation specifies successive hexadecimal fields of zero.**

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Example

```
DellEMC#show ipv6 pim rp
Group                                       RP
ff0e::225:1:1:1                             150::1
ff0e::225:1:1:2                             150::1
ff0e::225:1:1:4                             150::1
ff0e::225:1:1:5                             150::1
DellEMC#show run pim
!
ip pim bsr-candidate Loopback 0
ip pim vrf red bsr-candidate Loopback 1
ip pim vrf blue bsr-candidate Loopback 2
ip pim vrf red rp-candidate Loopback 1
ip pim vrf blue rp-candidate Loopback 2
ipv6 pim bsr-candidate Loopback 0
ipv6 pim vrf red bsr-candidate Loopback 1
ipv6 pim vrf blue bsr-candidate Loopback 2
ipv6 pim rp-candidate Loopback 0 100 def_vrf_acl
ipv6 pim vrf red rp-candidate Loopback 1 100 def_vrf_acl
ipv6 pim vrf blue rp-candidate Loopback 2 60 blue_vrf_acl_dut
DellEMC#
```

Example (Mapping)

```
DellEMC#show ipv6 pim rp mapping
PIM Group-to-RP Mappings
Group(s): ff0e::225:1:1:1/128
  RP: 100::1, v2
    Info source: 200::1, via bootstrap, priority 100
         expires: 00:01:50
```

```
  RP: 150::1, v2
    Info source: 200::1, via bootstrap, priority 100
         expires: 00:01:50
  RP: 200::1, v2
    Info source: 200::1, via bootstrap, priority 100
         expires: 00:01:57
Group(s): ff0e::225:1:1:2/128
  RP: 100::1, v2
    Info source: 200::1, via bootstrap, priority 100
         expires: 00:01:50
  RP: 150::1, v2
    Info source: 200::1, via bootstrap, priority 100
         expires: 00:01:50
  RP: 200::1, v2
    Info source: 200::1, via bootstrap, priority 100
         expires: 00:01:57
Group(s): ff0e::225:1:1:4/128
  RP: 100::1, v2
DellEMC#
```

show ipv6 pim summary

View information about PIM-SM operation.

Syntax

```
show ipv6 pim [vrf vrf-name] summary
```

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to configure this setting on that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Example

```
Dell# show ipv6 pim summary

PIM TIB version 1480
Uptime 5d4h
Entries in PIM-TIB/MFC : 105/81

Active Modes :
        PIM-SM

Interface summary:
        3 active PIM interfaces
        0 passive PIM interfaces
        2 active PIM neighbors

TIB summary:
        12/12 (*,G) entries in PIM-TIB/MFC
```

```
        69/69 (S,G) entries in PIM-TIB/MFC
        24/0 (S,G,Rpt) entries in PIM-TIB/MFC

        8 PIM nexthops
        1 RPs
        7 sources
        30 Register states

Message summary:
        47132/53793 Joins/Prunes sent/received
        0/0 Candidate-RP advertisements sent/received
        0/0 BSR messages sent/received
        0/0 MSDP updates sent/received
        243746/0 Null Register messages sent/received
        0/973809 Register-stop messages sent/received

Data path event summary:
        222 no-cache messages received
        281 last-hop switchover messages received
        26260/2958 pim-assert messages sent/received
        0/0 register messages sent/received
Dell#
```

show ipv6 pim tib

View the IPv6 PIM multicast-routing database (tree information base — tib).

Syntax `show ipv6 pim [vrf vrf-name] tib [group-address [source-address]]`

Parameters

vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view IP PIM debugging messages corresponding to that VRF. **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**
group-address	(OPTIONAL) Enter the multicast group address in the x:x:x:x::x format to view RP mappings for a specific group. **NOTE: The :: notation specifies successive hexadecimal fields of zero.**
source-address	(OPTIONAL) Enter the source address in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zero.**

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.3.0	Introduced on the Z9100-ON, S4048-ON, S6000-ON, S6100-ON, S4048T-ON, S3100, S6010-ON, S3048-ON, and C9010.

Example

```
Dell#show ipv6 pim tib

PIM Multicast Routing Table
Flags: D - Dense, S - Sparse, C - Connected, L - Local, P - Pruned,
       R - RP-bit set, F - Register flag, T - SPT-bit set, J - Join SPT,
       M - MSDP created entry, A - Candidate for MSDP Advertisement
       K - Ack-Pending State
Timers: Uptime/Expires
Interface state: Interface, next-Hop, State/Mode

(25::1, ff0e::225:1:2:1), uptime 00:09:53, expires 00:00:00,flags: CJ
  RPF neighbor: TenGigabitEthernet 1/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 2/11

(25::1, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00,flags: CJ
  RPF neighbor: TenGigabitEthernet 1/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/11

(25::2, ff0e::225:1:2:2), uptime 00:09:54, expires 00:00:00,flags: CJ
  RPF neighbor: TenGigabitEthernet 1/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/11

(25::1, ff0e::226:1:2:1), uptime 00:09:54, expires 00:00:00,flags: CJ
  RPF neighbor: TenGigabitEthernet 1/3, fe80::201:e8ff:fe00:6265
  Outgoing interface list:
    TenGigabitEthernet 1/11
Dell#
```

Related Commands clear ipv6 pim tib – clears the IPv6 PIM tree information base (TIB)

45

Policy-based Routing (PBR)

Policy-based routing (PBR) allows you to apply routing policies to specific interfaces. To enable PBR, create a redirect list and apply it to the interface. After the redirect list is applied to the interface, all traffic passing through the interface is subject to the rules defined in the redirect list. PBR is supported by the Dell Networking Operating System (OS).

You can apply PBR to physical interfaces and logical interfaces (such as a link aggregation group [LAG] or virtual local area network [VLAN]). Trace lists and redirect lists do not function correctly when you configure both in the same configuration.

NOTE: Apply PBR to Layer 3 interfaces only.

NOTE: For more information , refer to Content Addressable Memory (CAM) chapter.

Topics:

- ip redirect-group
- ip redirect-list
- permit
- redirect
- seq
- show cam pbr
- show ip redirect-list

ip redirect-group

Apply a redirect list (policy-based routing) on an interface. You can apply multiple redirect lists to an interface by entering this command multiple times.

C9000 Series

Syntax

`ip redirect-group` *`redirect-list-name`*

To remove a redirect list from an interface, use the `no ip redirect-group` *`name`* command.

Parameters

redirect-list-name	Enter the name of a configured redirect list.

Defaults none

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048–ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.2.0	Introduced on the E-Series TeraScale.
7.7.1.0	Introduced on the E-Series ExaScale.

Usage Information

You can apply any number of redirect-groups to an interface. A redirect list can contain any number of configured rules. These rules include the next-hop IP address where the incoming traffic is redirected.

If the next hop address is reachable, traffic is forwarded to the specified next hop. Otherwise, the normal routing table is used to forward traffic. When a redirect-group is applied to an interface and the next-hop is reachable, the rules are added into the PBR CAM region. When incoming traffic hits an entry in the CAM, the traffic is redirected to the corresponding next-hop IP address specified in the rule.

NOTE: Apply the redirect list to physical, VLAN, or LAG interfaces only.

Related Commands

- show cam pbr – displays the content of the PBR CAM.
- show ip redirect-list – displays the redirect-list configuration.

ip redirect-list

Configure a redirect list and enter REDIRECT-LIST mode.

C9000 Series

Syntax

`ip redirect-list` *`redirect-list-name`* `]`

To remove a redirect list, use the `no ip redirect-list` command.

Parameters

redirect-list-name	Enter a description to identify the IP redirect list (16 characters maximum)

Defaults

None

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048–ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.2.0	Introduced on the E-Series TeraScale.
7.7.1.0	Introduced on the E-Series ExaScale.

permit

Configure a permit rule. A permit rule excludes the matching packets from PBR classification and routes them using conventional routing.

C9000 Series

Syntax

`permit {`*`ip-protocol-number`* `|` *`protocol-type`*`} {`*`source mask`* `| any | host` *`ip-address`*`} {`*`destination mask`* `| any | host` *`ip-address`*`} [`*`bit`*`] [operators]`

To remove the rule, use one of the following:

- If you know the filter sequence number, use the `no seq` *`sequence-number`* `syntax` command.
- You can also use the `no permit {`*`ip-protocol-number`* `|` *`protocol-type`*`} {`*`source mask`* `| any | host` *`ip-address`*`} {`*`destination mask`* `| any | host` *`ip-address`*`} [`*`bit`*`] [operators]` command.

Parameters

ip-protocol-number	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
protocol-type	Enter one of the following keywords as the protocol type: • `icmp` for internet control message protocol • `ip` for any internet protocol • `tcp` for transmission control protocol • `udp` for user datagram protocol
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword `host` then he IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
bit	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags:

- `ack` = acknowledgement
- `fin` = finish (no more data from the user)
- `psh` = push function
- `rst` = reset the connection
- `syn` = synchronize sequence number
- `urg` = urgent field

operator (OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand:

- `eq` = equal to
- `neq` = not equal to
- `gt` = greater than
- `lt`= less than
- `range` = inclusive range of ports (you must specify two ports for the `port`command parameter.)

Defaults none

Command Modes REDIRECT-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048–ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.2.0	Introduced on the E-Series TeraScale.
7.7.1.0	Introduced on the E-Series ExaScale.

redirect

Configure a rule for the redirect list.

C9000 Series

Syntax `redirect {ip-address | slot/port} | tunnel tunnel-id}[track <obj-id>] {ip-protocol-number | protocol-type [bit]} {source mask | any | host ip-address} {destination mask | any | host ip-address} [operator]`

To remove this filter, use one of the following:

- Use the `no seq sequence-number` command if you know the filter's sequence number.
- You can also use the `no redirect {ip-address | slot/port}| tunnel tunnel-id}[track <obj-id>] {ip-protocol-number [bit] | protocol-type} {source mask | any |`

`host` *ip-address*} {*destination mask* | `any` | `host` *ip-address*} [*operator*] command.

Parameters

redirect Enter the keyword `redirect` to assign the sequence to the redirect list.

ip-address Enter the IP address of the forwarding router.

slot/port Enter the keyword `slot / port` then the slot/port information.

tunnel Enter the keyword `tunnel` to configure the tunnel setting.

tunnel-id Enter the keyword `tunnel-id` to redirect the traffic.

track Enter the keyword `track` to enable the tracking.

track <obj-id> Enter the keyword `track <obj-id>` to track object-id.

ip-protocol-number Enter a number from 0 to 255 for the protocol identified in the IP protocol header.

protocol-type Enter one of the following keywords as the protocol type:

- `icmp` for internet control message protocol
- `ip` for any internet protocol
- `tcp` for transmission control protocol
- `udp` for user datagram protocol

bit (OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags:

- `ack` = acknowledgement
- `fin` = finish (no more data from the user)
- `psh` = push function
- `rst` = reset the connection
- `syn` = synchronize sequence number
- `urg` = urgent field

source Enter the IP address of the network or host from which the packets were sent.

mask Enter a network mask in /prefix format (/x).

any Enter the keyword `any` to specify that all traffic is subject to the filter.

host *ip-address* Enter the keyword `host` then the IP address to specify a host IP address.

destination Enter the IP address of the network or host to which the packets are sent.

operator (OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand:

- `eq` = equal to
- `neq` = not equal to
- `gt` = greater than
- `lt` = less than
- `range` = inclusive range of ports (you must specify two ports for the`port` command parameter.)

Defaults none

Command Modes REDIRECT-LIST

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048–ON.
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Added support for the track-id on the S4810, S4820T, S6000, and Z9000.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
8.4.2.1	Introduced on the C-Series and S-Series.
8.4.2.0	Introduced on the E-Series TeraScale.
7.7.1.0	Introduced on the E-Series ExaScale.

seq

Configure a filter with an assigned sequence number for the redirect list.

C9000 Series

Syntax

```
seq sequence-number {permit | redirect {ip-address | tunnel tunnel-id}[track
<obj-id>] }} {ip-protocol-number | protocol-type} {source mask | any | host ip-
address} {destination mask | any | host ip-address} [bit] [operator]{source-
port source-port| source-port-range start-port - end-port} {destination-port
destination-port| destination-port-range start-port - end-port}
```

To delete a filter, use the `no seq sequence-number` command.

Parameters

sequence-number	Enter a number from 1 to 65535.
permit	Enter the keyword `permit` assign the sequence to the permit list.
redirect	Enter the keyword `redirect` to assign the sequence to the redirect list.
ip-address	Enter the keyword `IP address` of the forwarding router.
tunnel	Enter the keyword `tunnel` to configure the tunnel setting.
tunnel-id	Enter the keyword `tunnel-id` to redirect the traffic.
track	Enter the keyword `track` to enable the tracking.
track <obj-id>	Enter the keyword `track <obj-id>` to track object-id.
ip-protocol-number	Enter the keyword `ip-protocol-number` then the number from 0 to 255 for the protocol identified in the IP protocol header.

protocol-type	Enter one of the following keywords as the protocol type: • `icmp` for internet control message protocol • `ip` for any internet protocol • `tcp` for transmission control protocol • `udp` for user datagram protocol
source	Enter the IP address of the network or host from which the packets were sent.
mask	Enter a network mask in /prefix format (/x).
any	Enter the keyword `any` to specify that all traffic is subject to the filter.
host *ip-address*	Enter the keyword `host` then the IP address to specify a host IP address.
destination	Enter the IP address of the network or host to which the packets are sent.
bit	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: • `ack` = acknowledgement • `fin` = finish (no more data from the user) • `psh` = push function • `rst` = reset the connection • `syn` = synchronize sequence number • `urg` = urgent field
operator	(OPTIONAL) For the TCP and UDP parameters only. Enter one of the following logical operand: • `eq` = equal to • `neq` = not equal to • `gt` = greater than • `lt`= less than • `range` = inclusive range of ports (you must specify two ports for the port command parameter.)
source port	Enter the keywords `source-port` then the port number to be matched in the ACL rule in the ICAP rule
destination-port	Enter the keywords `destination-port` then the port number to be matched in the ACL rule in the ICAP rule.
source-port-range	Enter the keywords `Source-port-range` then the range of the start port to end port to be matched in the ACL rule in the ICAP rule.
destination-port-range	Enter the keywords `destination-port-range` then the range of the start port to end port to be matched in the ACL rule in the ICAP rule.

Defaults none

Command Modes REDIRECT-LIST

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.8(0.0)	Introduced on the S3048-ON and S4048–ON.
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Added support for the track-id on the S4810, S4820T, S6000, and Z9000.
9.5(0.1)	Introduced on the Z9500
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

show cam pbr

Display the PBR CAM content.

C9000 Series

Syntax

```
show cam pbr {[interface interface] | linecard slot-number port-set number]}
[summary]
```

Parameters

interface *interface*	Enter the keyword `interface` then the name of the interface.
linecard *number*	Enter the keyword `linecard` then the slot number. The range is from 0 to 11.
port-set *number*	Enter the keywords `port-set` then the port-pipe number.
summary	Enter the keyword `summary` to view only the total number of CAM entries.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048–ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information The `show cam pbr` command displays the PBR CAM content.

Related Commands

- ip redirect-group – applies a redirect group to an interface.
- show ip redirect-list – displays the redirect-list configuration.

show ip redirect-list

View the redirect list configuration and the interfaces it is applied to.

C9000 Series

Syntax `show ip redirect-list redirect-list-name`

Parameters

redirect-list-name	Enter the name of a configured Redirect list.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048–ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Example

```
Dell#sh ip redirect-list
IP redirect-list test1:
Defined as:
  seq 5 redirect tunnel 1 track 1 ip any any, Track 1 [up], Next-hop reachable
(via Te 0/7)
Applied interfaces:
  Vl 200
Dell#
```

46

Port Extenders (PE)

To configure a C1048P port extender (PE) attached to a C9010, use the commands in this chapter from the C9010 console.

Important Points to Remember

- You can perform the following tasks using the commands described in this chapter:
  - Provisioning a Port Extender
  - Managing a Port Extender
  - PE Stacking
- You must configure the `feature extended-bridge` command to turn on support for PE configuration on a C9010.
- The GVRP and FRRP protocols are not supported on the PE ports.

NOTE: Dell Networking OS recommends not to use RPM Slots 10 and 11 for PE connectivity.

For information on the commands you can enter from a PE console to configure a port extender, see the *PE Console* chapter.

For information on using the PE features, see the "Port Extenders" chapter in the *Dell Networking OS Configuration Guide for the C9000 Series*.

Topics:

- cascade interface
- clear pe statistics
- connect pe
- feature extended-bridge
- location-led
- pe
- pe provision
- pe-version-compat-support
- reset pe schedule
- reset pe range
- reset pe schedule show
- reset pe unschedule
- show config
- show ecid
- show pe
- show pe csp
- show pe errors
- Dual Homing
- Debugging
- Power over Ethernet (PoE)

cascade interface

Configure an interface as a cascade interface.

C9000 Series

Syntax

```
cascade interface interface slot/port-range [peer]
```

Parameters

interface *interface*	Enter `interface` and specify the interface supported on the switch. The TenGigabit Ethernet interface is the only interface type supported for this feature.
slot/port-range	Enter the *slot/port-range* to specify a linecard and either a single port number, a port range, or a combination of both for auto-LAG configuration. Slot number range is from 0 to 9. In linecard slots 0 to 9, the range of port numbers is from 0 to 23.
peer	Enter `peer` to configure the VLT peer in a dual-homing setup. This parameter is available only in the Configuration Terminal Batch Mode.

Default

None

Command Modes

PE CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command-Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode and the `peer` parameter on C9010.
9.9(0.0)	Introduced on the C9010.

Usage Information

This command provisions the port extender for automatic link aggregation group (LAG) port channel creation on the connected ports. The LAG member ports must be operationally up and have a default port configuration with no Layer 2 and Layer 3 configuration. The port interfaces must be of the same type. You can configure up to 16 switch ports in the auto-LAG.

Use `cascade interface interface slot/port-range peer` in the Configuration Terminal Batch Mode to provision the port extender in a dual-homing setup. It is recommended to configure the port extender through batch mode only in a dual-homing setup. If the peer is not connected during the configuration, ensure that you import the configuration from the peer once it is up. See import peer-config.

- The *slot/port-range* specifies a line card and either a single port number, a port range, or a combination of both for auto-LAG configuration. The range of slot numbers is from 0 to 9 for linecard slots. The range of port numbers is from 0 to 23.

Example

PE Configuration Mode

```
Dell(conf)# feature extended-bridge
Dell(conf)# pe provision 4
Dell(conf-pe-4)#cascade interface tengigabitethernet 1/1-2
```

Configuration Terminal Batch Mode

```
Dell#conf terminal batch
Peer is registered
Dell(conf-b)#pe provision 4
Dell(conf-b-pe-4)#cascade interface tengigabitethernet 1/1-2
```

clear pe statistics

Delete the statistics related to a specified port extender.

C9000 Series

Syntax `clear pe pe-id statistics`

Parameters

pe-id	Enter the keyword `pe` and the port extender ID. Range is from 0 to 255.
statistics	Enter the keyword `statistics` to delete the statistics related to a specified PE from the system.

Default None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Example

```
Dell#clear pe 4 statistics
```

connect pe

Connect to a port extender (PE) through Telnet.

C9000 Series

Syntax `connect pe pe-id`

Parameters

pe-id Enter the keyword `pe` and the port extender ID. Range is from 0 to 255.

Default

None

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

You can connect to an attached PE through Telnet using the `connect pe` command and view information specific to the PE system. After you log in to a port extender, enter `?` or `help` to display a list of supported commands.

Example

```
Dell#connect pe 254
Login: peadmin
Password:
DellPE>
```

feature extended-bridge

Enable 802.1BR (bridge port extender) support on the switch.

C9000 Series

Syntax

`[no] feature extended-bridge`

To disable 802.1BR support on the switch, use the `no feature extended-bridge` command.

Default

None

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

This command enables support for the 802.1 bridge PE (BR) on the switch. Enabling the PE feature allows you to provision the PE. The `no feature extended-bridge` command disables bridge PE support and deprovisions a PE. When you use this command in the Configuration Terminal Batch mode, you can enable the support for the bridge PE connected in a Dual-Homing setup.

You can use the `show feature` command to check whether the extended-bridge feature has been enabled as shown in the following example.

Example

```
Dell>show feature
Feature                  State
-------                  -----
VRF                      disabled
Extended-Bridge          enabled
```

Related Commands pe provision — Logically provision or add a PE.

location-led

Toggle the location LED of a specified interface, linecard or port extender (PE) on or off.

C9000 Series

Syntax `location–led {interface` *`interface`* `| linecard` *`slot-id`* `| pe` *`pe-id`* `stack-unit` *`unit-number`* `| rpm` *`slot-id`* `}{off|on}`

Parameters

interface *interface*	Enter the following keywords and slot/port or number information: • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a Gigabit Ethernet interface, enter the keyword `gigabitethernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
linecard *slot-id*	Enter the keyword `linecard` and the slot ID. The linecard *slot-id* range is from 0 to 9.
pe *pe-id*	Enter the keyword `pe` and the PE ID. The range is from 0 to 255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the stack unit number. The range is from 0 to 7.
rpm *slot-id*	Enter the keyword `rpm` and specify the route processor slot ID. RPM slot-id values are *rpm0* and *rpm1* .
on |off	Turn the location LED(s) of the specified interfaces, linecard, port extenders (PE), ports and RPMs on or off.

Default None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information When the location LED setting is turned "on" for a port extender (PE), the main power supply LED on the PE flashes green light and when the location LED setting is turned "off", the main power supply LED is in a solid green state.

The`location-led` settings are not saved through power cycles if the C1048 system is power cycled.

Example

```
Dell#
Dell#location-led pe 255 stack-unit 0 on
```

pe

Add a pre-provisioned port extender (PE) .

C9000 Series

Syntax `pe pe-id`

To remove a port extender, use the `no pe pe-id` command.

Parameters

pe *pe-id*	Enter keyword `pe` and PE ID. The range is from 0 to 255.

Default None

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information The `pe pe-id` command adds a pre-provisioned PE. The port extender ID (*pe-id*) range is from 0 to 255. You can add a port extender stack-unit using `stack-unit unit number` keyword.

To remove a port extender, use the `no pe pe-id` command.

Example

```
Entering pe context
DELL(conf)# pe 0

Removing pe 0
DELL(conf)# no pe 0

Entering port extender configuration mode:
DELL(conf)#pe 10
DELL(conf-pe-10)#
DELL(conf-pe-10)#stack-unit 0 type c1048P
```

Related Commands

- stack-unit – add or delete a specified port extender stack-unit.
- show pe —display the port extender status and details.

pe provision

Logically provision or add a port extender (PE).

C9000 Series

Syntax

`pe provision` *`pe-id`*

To de-provision or delete a port extender, use the `no pe provision` *`pe-id`* command.

Parameters

pe provision ***pe-id***	Enter port-extender configuration mode to logically provision a port extender. Port extender ID range is from 0 to 255

Default

None

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(2.0P2)	Introduced the PE description and stack-unit description options.
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.

Usage Information

Before you provision a port extender, enable the extended bridge feature using the `feature extended-bridge` command. The `pe provision` *`pe-id`* command logically pre-provisions or adds a port extender (PE) even when the PE is not physically connected to the switch. The port extender ID (*pe-id*) range is from 0 to 255.

After provisioning a PE using the `pe provision pe-id` , you can provision a stack unit using the `stack-unit` command.

You can also add a PE description and stack-unit description using the `description name` and the `stack-unit 0 description name` commands respectively.

You can provision a port extender connected in a Dual-Homing setup from the Configuration Terminal Batch mode.

To de-provision a port extender, use the `no pe provision pe-id` command.

NOTE: You must ensure that the port extender units are offline before you issue the `no pe provision` command.

Example

```
DELL(conf)# pe provision 10
DELL(conf-pe-10)#

DELL(conf)# no pe provision 10
```

```
DELL(conf)# pe provision 0
DELL(conf-pe-0)# stack-unit 0 type N2048-PE
DELL(conf-pe-0)# stack-unit 1 type N2024P-PE
DELL(conf-pe-0)# cascade interface TenGigabitEthernet 0/14-15
DELL(conf-pe-0)# description Test
DELL(conf-pe-0)# stack-unit 0 description first
DELL(conf-pe-0)# stack-unit 1 description second
```

Related Commands

- feature extended-bridge
- stack unit
- show pe

pe-version-compat-support

Enables the scheduled PE reboot feature.

Syntax `pe-version-compat-support enable`

Defaults Enable.

Parameters

enable	Enter the keyword `enable` to turn on the scheduled PE reboot feature.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010.

Usage Information This command adds an entry to the startup-config file. Once this feature is enabled, it is available for all PEs.

reset pe schedule

Configure the PEs to reset or reboot at a specified period of time.

Syntax

```
reset pe schedule {after HHHH:MMMM | at [HHHH:MMMM-DD:MM:YR | HHHH:MMMM]}
{range pe-id-pe-id}
```

Defaults

None.

Parameters

after *HHHH:MMMM*	Enter the keyword `after` followed by the amount of time in hours and minutes after which the PEs should reboot.
at *HHHH:MMMM*	Enter the keyword `at` followed by the exact time on the current date at which the PEs should reboot.
at *HHHH:MMMM-DD:MM:YR*	Enter the keyword `at` followed by the exact date and time at which the PEs should reboot.
range *pe-id-pe-id*	Enter the keyword `range` followed by the range of pe-ids that you want to schedule to reboot. The range is from 0 to 255.

Command Modes

- EXEC Privilege

Usage Information

- You can schedule a PE to reboot after a particular amount of time, in hours and minutes (HH:MM), from the current time. For example, you can schedule a PE to reset 10 minutes from the current time using the following command: `reset pe schedule after 0:10 range 10-20`.
- You can schedule a PE to reset exactly at the specific date and time. For example, you can schedule a PE to reset at a 0:10 PM on 29th November 2017 using the following command: `reset pe schedule at 0:10-11/29/17 range 10-20`.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010.

reset pe range

Specify a range of port extenders (PEs) that you want to schedule for rebooting at a later point of time.

Syntax

```
reset pe range {pe-id-pe-id | pe-id1,pe-id2,.......} {no-confirm}
```

Defaults

None.

Parameters

pe-id-pe-id	Enter the range of port extender IDs that you want to schedule for rebooting.
pe-id1,pe-id2,.....	Enter a list of port extender IDs that you want to schedule for rebooting with each pe-id delimited by a coma.

no-confirm	Enter the keyword `no-confirm` to suppress the warning messages that are displayed during rebooting of the PE.

Command Modes

- EXEC Privilege

Usage Information

- The `reset pe range` command is applicable for the entire PE stack-unit. This command is not used for per stack-unit scenario.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13(0.0)	Added the `range` keyword to the command.
9.9(0.0)	Introduced on the C9010.

Example

The following command resets all the PEs within range 1 to 5: `reset pe range 1-5 no-confirm`.

The following command resets all the PEs within range 5 to 10 and also the pe-ids 1 and 3: `reset pe range 1,3,5-10 no-confirm`.

reset pe schedule show

Display a list of PEs that are scheduled to be rebooted.

Syntax `reset pe schedule show`

Defaults None.

Command Modes

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010.

Example

```
JobID  Status          Scheduled Start Time        Scheduled PE's
  000  Scheduled        08:59-09/19/17                   0,1
  001  Scheduled        23:30-09/19/17                   2,3
  002  Scheduled        20:30-12/29/17                   5-6
```

reset pe unschedule

Use this command to undo the scheduled PR reboot configuration.

Syntax `reset pe unschedule job-id`

Defaults None.

Parameters

job-id	Enter the job ID of the scheduled PE reboot configuration that you want to undo.

Command Modes

- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010.

show config

Display the PE provision configuration details.

C9000 Series

Syntax `show config`

Command Modes PE CONFIG (conf-pe-*pe-id*)

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Example

```
Dell(conf-pe-5)# show config
!
pe provision 5
 stack-unit 4 type C1048P
```

```
Dell(conf)#pe 255
Dell(conf-pe-255)#show config
!
pe provision 255
 cascade interface TenGigabitEthernet 6/0
 stack-unit 1 type C1048P
```

show ecid

Display the E-Channel identifier (ECID) information for all or any specified interfaces.

C9000 Series

Syntax

```
show ecid {interface [interface] | pe pe-id stack–unit unit-number}
```

Parameters

interface *interface*	Enter the `interface` keyword, and specify one of the following *interface* types: • For a PE Gigabit Ethernet interface, enter the keyword `peGigE`. You must specify a *pe-id/stack-unit/port-id* for the interface. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE. • For a port channel interface, enter the keyword `port-channel` • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
pe *pe-id*	Enter the keyword `pe` keyword and specify a port extender ID number. Range is from 0 to 255.
stack-unit *unit-number*	Enter the keyword `stack-unit` and the unit number. Range is from 0 to 7.

Default

None

Command Modes

EXEC

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.14(0.0)	Added the SVP (Source Virtual Port) information also along with E-Channel identifier (ECID) information.
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.

Usage Information

Use the `show ecid` command to view the E-Channel Identifier (ECID) information for a specified interface such as a port extender Gigabit Ethernet (peGigE) interface.

Example

```
DellEMC#show ecid pe 255
-------------------------------------
Interface           ECID       SVP
```

```
-----------------------------------
Port-channel 513    3225       8022
peGigE 255/0/1      3226       8023
peGigE 255/0/2      3227       8024
peGigE 255/0/3      3228       8025
peGigE 255/0/4      3229       8026
peGigE 255/0/5      3230       8027
peGigE 255/0/6      3231       8028
peGigE 255/0/7      3232       8029
peGigE 255/0/8      3233       8030
peGigE 255/0/9      3234       8031
peGigE 255/0/10     3235       8032
peGigE 255/0/11     3236       8033
peGigE 255/0/12     3237       8034
peGigE 255/0/13     3238       8035
peGigE 255/0/14     3239       8036
peGigE 255/0/15     3191       8037
peGigE 255/0/16     3241       8038
peGigE 255/0/17     3242       8039
peGigE 255/0/18     3243       8040
peGigE 255/0/19     3244       8041
peGigE 255/0/20     3245       8042
peGigE 255/0/21     3246       8043
peGigE 255/0/22     3247       8044
peGigE 255/0/23     3248       8045
peGigE 255/0/24     3249       8046
peGigE 255/0/25     3250       8047
peGigE 255/0/26     3251       8048
peGigE 255/0/27     3252       8049
peGigE 255/0/28     3253       8050
peGigE 255/0/29     3254       8051
peGigE 255/0/30     3255       8052
peGigE 255/0/31     3256       8053
peGigE 255/0/32     3257       8054
peGigE 255/0/33     3258       8055
peGigE 255/0/34     3259       8056
peGigE 255/0/35     3260       8057
peGigE 255/0/36     3261       8058
peGigE 255/0/37     3262       8059
peGigE 255/0/38     3263       8060
peGigE 255/0/39     3264       8061
peGigE 255/0/40     3265       8062
peGigE 255/0/41     3266       8063
peGigE 255/0/42     3267       8064
peGigE 255/0/43     3268       8065
peGigE 255/0/44     3269       8066
peGigE 255/0/45     3270       8067
peGigE 255/0/46     3271       8068
peGigE 255/0/47     3272       8069
peGigE 255/0/48     3273       8070
peTenGigE 255/0/49  3755       8299
peTenGigE 255/0/50  3754       8298
peGigE 255/1/1      3466       8263
peGigE 255/1/2      3467       8264
peGigE 255/1/3      3468       8265
peGigE 255/1/4      3469       8266
peGigE 255/1/5      3470       8267
peGigE 255/1/6      3471       8268
peGigE 255/1/7      3472       8269
peGigE 255/1/8      3473       8270
peGigE 255/1/9      3474       8271
peGigE 255/1/10     3475       8272
peGigE 255/1/11     3476       8273
peGigE 255/1/12     3477       8274
peGigE 255/1/13     3478       8275
peGigE 255/1/14     3479       8276
peGigE 255/1/15     3480       8277
peGigE 255/1/16     3481       8278
peGigE 255/1/17     3482       8279
```

```
peGigE 255/1/18     3483       8280
peGigE 255/1/19     3484       8281
peGigE 255/1/20     3436       8282
peGigE 255/1/21     3739       8283
peGigE 255/1/22     3740       8284
peGigE 255/1/23     3741       8285
peGigE 255/1/24     3742       8286
peTenGigE 255/1/25  3757       8301
peTenGigE 255/1/26  3758       8302
peGigE 255/7/1      3442       8239
peGigE 255/7/2      3443       8240
peGigE 255/7/3      3444       8241
peGigE 255/7/4      3445       8242
peGigE 255/7/5      3446       8243
peGigE 255/7/6      3447       8244
peGigE 255/7/7      3448       8245
peGigE 255/7/8      3449       8246
peGigE 255/7/9      3450       8247
peGigE 255/7/10     3451       8248
peGigE 255/7/11     3452       8249
peGigE 255/7/12     3453       8250
peGigE 255/7/13     3454       8251
peGigE 255/7/14     3455       8252
peGigE 255/7/15     3456       8253
peGigE 255/7/16     3457       8254
peGigE 255/7/17     3458       8255
peGigE 255/7/18     3459       8256
peGigE 255/7/19     3460       8257
peGigE 255/7/20     3461       8258
peGigE 255/7/21     3462       8259
peGigE 255/7/22     3463       8260
peGigE 255/7/23     3464       8261
peGigE 255/7/24     3465       8262
peTenGigE 255/7/26  3756       8300
```

show pe

Display the port extender status and details including the PE description.

C9000 Series

Syntax `show pe [pe-id | brief | statistics]`

Parameters

pe-id	(Optional) Enter the port extender ID number *pe-id* to display the status and details of a specified port extender.
brief	(Optional) Enter the keyword `brief` to display all the port extender information in brief.
statistics	(Optional) Enter the keyword `statistics` to display all the port extender statistics.

Default None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.14(0.0)	Enhanced to include maximum number of PEX ports information to appear in the display content.
9.13(0.1)	Added the port validation error (PVE) status information to appear in the display content. Added the online and offline PE and PE unit count information to appear in the display content.
9.13(0.0)	Added the Software Version Compatibiy (SVC) status information to appear in the display content.
9.11(2.0P2)	Enhanced to include the PE description field.
9.9(0.0)	Introduced on the C9010.

Usage Information

This command shows the current number of PEs in the system that are online and the current number of PEs that are offline. This command also shows the port validation error (PVE) to indicate that the number of PEX ports have exceeded the maximum limit. The PVE error results from an incorrect provisioning of PEs or misconfiguration of converted uplink ports in the dual homed system. All the PE units in the secondary VLT node are shown to be in PVE state.

Example

```
Dell#show pe
Maximum number of PE Units allowed: 80
Current number of PE units in the system: 7 (Online: 5 Offline: 2)
Current number of PEs in the system: 3 (Online: 2 Offline: 1)
Current number of PEX ports in the system: 288 (Maximum: 4000)

Codes:  A - Active, I - Inactive
        SVC - Software Version Compatible
Reason: CTM - Card Type Mismatch, CAM - CAM ACL Mismatch
        SVM - Software Version Mismatch, UE - Unknown Error
Offline Reason: UNP - Unit Not Present,  PVE - Port Validation Error
                ICE - IPC CP Error, IRE - IPC RP Error
                ISE - IPC Setup Error, CVE - Card Validation Error

PE-ID assigned: 0
Status: offline
System Mac: f4:8e:38:23:7c:c7
PE Up Time: 00:00:00
PE Description:
PE Discovery Status: Provisioned PE
User Configured Cascade Ports: None
Cascade LAG: Po 258, Local Status: Down, Remote Status: Down
PE Configuration: Local Status: Present, Remote Status: Not Present
-------------------------------------------------------------------------------
Stack-id  Status    Reason  Type        UnitMac        No. of Ports  Description
-------------------------------------------------------------------------------
    0     offline   UNP     N3024P-PE  00:00:00:00:00:00    30
    1     offline   UNP     N2048-PE   00:00:00:00:00:00    52

PE-ID assigned: 1
Status: online
System Mac: f8:b1:56:73:a2:91
PE Up Time: 02:56:05
PE Description:
PE Discovery Status: Provisioned PE
User Configured Cascade Ports: Te 0/16(A)
Cascade LAG: Po 259, Local Status: Up, Remote Status: Down
PE Configuration: Local Status: Present, Remote Status: Not Present
-------------------------------------------------------------------------------
Stack-id  Status    Reason  Type        UnitMac        No. of Ports  Description
-------------------------------------------------------------------------------
    0     online    -       N2048P-PE  f8:b1:56:73:a2:91    52
    1     online    -       N2048P-PE  f8:b1:56:73:a2:89    52
    2     online    -       N3024P-PE  f4:8e:38:02:b1:43    30
```

```
PE-ID assigned: 255
Status: online
System Mac: f8:b1:56:33:ee:f2
PE Up Time: 02:56:12
PE Description:
PE Discovery Status: Provisioned PE
User Configured Cascade Ports: Te 0/21(A)
Cascade LAG: Po 513, Local Status: Up, Remote Status: Down
PE Configuration: Local Status: Present, Remote Status: Not Present
```

```
-------------------------------------------------------------------------------
Stack-id   Status Reason  Type      UnitMac          No. of Ports Description
-------------------------------------------------------------------------------
     0     online   -    N2048P-PE  f8:b1:56:73:87:f9   52        First
     1     online   -    N2048P-PE  f4:8e:38:04:f2:67   28        Second
Dell#
Dell#show pe 1 brief
           --  Port Extenders Information  --
-------------------------------------------------------------------------
  PE-id  Status  Stack-size  Type      System-MAC        Description
-------------------------------------------------------------------------
    255  online    2        N3048-PE  f8:b1:56:33:ee:f2

Dell#show pe statistics
PE-ID: 0
PE-CSP Tx Message: 0
PE-CSP Rx Message: 0
ECP Tx: 0
ECP Rx Ack: 0
ECP Dropped: 0
ECP Rx: 0
ECP Tx Ack: 0

PE-ID: 1
PE-CSP Tx Message: 10
PE-CSP Rx Message: 5
ECP Tx: 11
ECP Rx Ack: 11
ECP Dropped: 0
ECP Rx: 6
ECP Tx Ack: 6

PE-ID: 255
PE-CSP Tx Message: 9
PE-CSP Rx Message: 5
ECP Tx: 10
ECP Rx Ack: 10
ECP Dropped: 0
ECP Rx: 6
ECP Tx Ack: 6
Dell#
```

```
Dell#show pe 1
Codes:  A - Active, I - Inactive
        SVC - Software Version Compatible
Reason: CTM - Card Type Mismatch, CAM - CAM ACL Mismatch
        SVM - Software Version Mismatch, UE - Unknown Error
Offline Reason: UNP - Unit Not Present,  PVE - Port Validation Error
                ICE - IPC CP Error, IRE - IPC RP Error
                ISE - IPC Setup Error, CVE - Card Validation Error

PE-ID assigned: 1
Status: online
System Mac: f8:b1:56:73:a2:91
PE Up Time: 03:00:27
PE Description:
PE Discovery Status: Provisioned PE
User Configured Cascade Ports: Te 0/16(A)
Cascade LAG: Po 259, Local Status: Up, Remote Status: Down
```

```
PE Configuration: Local Status: Present, Remote Status: Not Present
-------------------------------------------------------------------------------
Stack-id  Status  Reason   Type       UnitMac      No. of Ports  Description
-------------------------------------------------------------------------------
    0     online    -     N2048P-PE  f8:b1:56:73:a2:91    52
    1     online    -     N2048P-PE  f8:b1:56:73:a2:89    52
    2     online    -     N3024P-PE  f4:8e:38:02:b1:43    30
Dell#
```

show pe csp

Display the control and status protocol (CSP) session information for the port extenders.

C9000 Series

Syntax `show pe CSP`

Default None

Command Modes

- EXEC
- EXEC Privileged

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

The following example displays the CSP session information for the port extenders. The command output shows the following information:

- `TxPDUSemStatus` shows the next port extender CSP PDU TX state machine status.
- `RxPDUSemStatus` shows the last port extender CSP PDU RX state machine status.
- `LocalReqSemStatus` shows the port extender CSP local request state machine status.
- `RemoteReqSemStatus` shows the port extender CSP remote request state machine status

Example

```
Dell#show pe csp
       --  Port Extenders CSP Information  --
-------------------------------------------------------------------------
  PE-id  TxPDUSemStatus  RxPDUSemStatus  LocalReqSemStatus  RemoteReqSemStatus
-------------------------------------------------------------------------
    254         WAIT_TX         WAIT_RX        RESP_RECVED           SEND_RESP
```

show pe errors

Display the port extender error logs.

C9000 Series

Syntax

```
show pe errors
```

Default

None

Command Modes

- EXEC
- EXEC Privileged

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

In the following example, the Te 1/16 is added as a cascade interface in PE 9, but Te1/16 is connected to a different PE, which is not provisioned. Hence, the cascade interface is kept in error state.

Example

```
Dell#show pe errors
PE-id: Not Assigned
PE MAC: f8:b1:56:00:01:04
Interface Errors:
   TenGigabitEthernet 1/16 - Error State

Dell#show pe 9
Codes:  A - Active, I - Inactive
        SVC - Software Version Compatible
Reason: CTM - Card Type Mismatch, CAM - CAM ACL Mismatch
        SVM - Software Version Mismatch, UE - Unknown Error
Offline Reason: UNP - Unit Not Present,  PVE - Port Validation Error
                ICE - IPC CP Error, IRE - IPC RP Error
                ISE - IPC Setup Error, CVE - Card Validation Error

PE-ID assigned: 9
Status: online
System Mac: f8:b1:56:00:01:28
PE Up Time: 08:36:56
PE Discovery Status: Provisioned PE
User Configured Cascade Ports: Te 1/9(A),Te 1/16(I)
Cascade LAG: Po 267(Up)
-----------------------------------------------------------------------
Stack-id   Status   Reason    Type     UnitMac         No. of Ports
-----------------------------------------------------------------------
    0      online    -        C1048P  f8:b1:56:00:02:24     52
    1      online    -        C1048P  f8:b1:56:00:01:28     52
    2      online    -        C1048P  f8:b1:56:00:01:90     52
    3      online    -        C1048P  00:00:ab:00:00:2c     52
```

Dual Homing

Use the commands in the following section to setup the configurations on a port extender connected in a dual-homing environment.

batch-write-memory

Saves the running configuration in both the VLT peers.

Syntax `batch-write-memory`

Parameters None

Defaults None

Command Modes CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13(0.0)	Introduced on the C9010.

Usage Information If the batch-write-memory command fails on one of the VLT peers, it does not affect the operation in the other VLT peer. Instead, an appropriate error message is displayed.

Example Primary VLT

```
DellEMC(conf-b)#batch-write-mem
DellEMC(conf-b)#Dec  6 11:33:35 %RPM1-P:CP %FILEMGR-5-FILESAVED: Copied
running-config to startup-config in flash by default
Dec  6 11:33:36 %RPM1-P:CP %CLIBATCH-6-CLIBATCH_PEER_CONFIG_WRITE_COMPLETE:
Copy of running-config to startup-config in VLT peer flash is successful
```

Secondary VLT

```
DellEMC#Dec  6 10:44:31 %RPM1-P:CP %CLIBATCH-6-
CLI_BATCH_CONFIG_IN_PROGRESS_TRAP: Batch configuration commit is in progress
Dec  6 10:44:31 %RPM1-P:CP %CLIBATCH-6-CLI_BATCH_CONFIG_COMPLETE_TRAP: Batch
configuration commit is success
Dec  6 10:44:31 %RPM1-P:CP %FILEMGR-5-FILESAVED: Copied running-config to
startup-config in flash by default
Dec  6 10:46:08 %RPM1-P:CP %FILEMGR-5-FILESAVED: Copied running-config to
startup-config in flash by default
```

commit

Use `commit` to apply the common configurations made in the Configuration Terminal Batch mode.

C9000 Series

Syntax `commit`

Default None

Command Modes CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the C9010.

Usage Information The Configuration Terminal Batch mode is used to setup common configurations on a port extender connected in a dual-homing environment. Use the `commit` command to apply the configuration changes. In the Configuration Terminal Batch mode, you can continue to commit the changes without exiting the batch mode.

Example Example with multiple Commits:

```
Dell#configure terminal batch
Peer is registered
Dell(conf-b)#interface peGigE 184/0/1
Dell(conf-b-if-pegi-184/0/1)#no shutdown
Dell(conf-b-if-pegi-184/0/1)#commit
Dell(conf-b)#Apr 5 06:48:28: %RPM1-P:CP %CLIBATCH-6-
CLI_BATCH_CONFIG_IN_PROGRESS_TRAP: Batch configuration commit is in progress
Apr 5 06:48:28: %RPM1-P:CP %IFMGR-5-ASTATE_UP: Changed interface Admin state
to up: PeGi 184/0/1
Apr 5 06:48:28: %RPM1-P:CP %CLIBATCH-6-CLI_BATCH_CONFIG_COMPLETE_TRAP: Batch
configuration commit is success

Dell(conf-b)#interface peGigE 184/0/1
Dell(conf-b-if-pegi-184/0/1)#switchport
Dell(conf-b-if-pegi-184/0/1)#int vla 1000
Dell(conf-b-if-vl-1000)#tagged peGigE 184/0/1
Dell(conf-b-if-vl-1000)#commit
Dell(conf-b)#Apr 5 06:48:47: %RPM1-P:CP %CLIBATCH-6-
CLI_BATCH_CONFIG_IN_PROGRESS_TRAP: Batch configuration commit is in progress
Apr 5 06:48:47: %RPM1-P:CP %IFMGR-5-ACTIVE: Changed Vlan interface state to
active: Vl 1000
Apr 5 06:48:48: %RPM1-P:CP %CLIBATCH-6-CLI_BATCH_CONFIG_COMPLETE_TRAP: Batch
configuration commit is success
```

commit write

Use `commit write` to apply the common configurations made in the Configuration Terminal Batch mode and to save the running configuration in both VLT peers.

C9000 Series

Syntax `commit write`

Parameters None

Default None

Command Modes CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010.

Usage Information

The Configuration Terminal Batch mode is used to setup common configurations on a port extender connected in a dual-homing environment. Use the `commit write` command to apply the configuration changes. It also saves the running configuration to the startup configuration in both VLT peers. In the Configuration Terminal Batch mode, you can continue to commit the changes without exiting the batch mode.

NOTE: If the `commit write` command fails on one VLT peer, your configuration is not applied on both VLT peers.

Example

Primary VLT

```
DellEMC(conf-b)#int range Tengigabitethernet 3/0 - 5
DellEMC(conf-if-range-te-3/0-5)#mtu 3500
DellEMC(conf-if-range-te-3/0-5)#exit
DellEMC(conf-b)#show conf
interface range tengigabitethernet 3/0 - 5
mtu 3500
DellEMC(conf-b)#commit write
DellEMC(conf-b)#Dec  6 11:31:58 %RPM1-P:CP %CLIBATCH-6-
CLI_BATCH_CONFIG_IN_PROGRESS_TRAP: Batch configuration commit is in progress
Dec  6 11:31:58 %RPM1-P:CP %FILEMGR-5-FILESAVED: Copied running-config to
startup-config in flash by default
Dec  6 11:31:59 %RPM1-P:CP %CLIBATCH-6-CLI_BATCH_CONFIG_COMPLETE_TRAP: Batch
configuration commit is success
Dec  6 11:31:59 %RPM1-P:CP %CLIBATCH-6-CLIBATCH_PEER_CONFIG_WRITE_COMPLETE:
Copy of running-config to startup-config in VLT peer flash is successful
```

Secondary VLT

```
DellEMC#Dec  6 10:44:31 %RPM1-P:CP %CLIBATCH-6-
CLI_BATCH_CONFIG_IN_PROGRESS_TRAP: Batch configuration commit is in progress
Dec  6 10:44:31 %RPM1-P:CP %CLIBATCH-6-CLI_BATCH_CONFIG_COMPLETE_TRAP: Batch
configuration commit is success
Dec  6 10:44:31 %RPM1-P:CP %FILEMGR-5-FILESAVED: Copied running-config to
startup-config in flash by default
```

Related Commands

- commit — apply the common configuration changes made in the Configuration Terminal Batch mode.

discard

Use the `discard` command to cancel the uncommitted changes made to common configurations in the Configuration Terminal Batch mode.

C9000 Series

Syntax `discard`

Default None

Command Modes CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the C9010.

Usage Information The Configuration Terminal Batch mode is used to setup common configurations on a port extender connected in a dual-homing environment. Use the `discard` command to cancel the uncommitted common configuration changes.

Example The following example shows the configurations being discarded:

```
Dell(conf-b)#interface vlan 2000
Dell(conf-b-if-vl-2000)#tagged peGigE 184/0/1
Dell(conf-b-if-vl-2000)#show config
interface vlan 2000
tagged peGigE 184/0/1

Dell(conf-b-if-vl-2000)#discard
Dell(conf-b)#show config
Dell(conf-b)#exit
Dell#
```

import peer-config

Use `import peer-config` to import the common configurations from the peer chassis.

C9000 Series

Syntax `import peer-config`

Default None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the C9010.

Usage Information Use the `import peer-config` to import the common configurations from the peer chassis and apply them in the local system.

show config-mismatch

Use `show config-mismatch` to view the configurations that differ between the peer chassis.

C9000 Series

Syntax `show config-mismatch`

Default None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the C9010.

Usage Information Use the `show config-mismatch` command to view the configurations in the local that do not match with the peer chassis.

show running-config local

Use `show running-config local` to view the local configurations.

C9000 Series

Syntax `show running-config local`

Default None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the C9010.

Usage Information Use `show running-config local` to view only the configurations corresponding to the local chassis.

Example

```
Dell#show running-config local
Current Configuration ...
! Version 1-0(0-4370)
```

```
! Last configuration change at Tue Nov  3 09:56:27 2015 by default
!
boot system rpm0 primary tftp://10.16.127.35/sys-vg-2
boot system rpm0 secondary tftp://10.16.127.36/sys-vg-2
boot system rpm0 default system: A:
boot system rpm1 primary tftp://10.16.127.35/sys-vg-2
boot system rpm1 secondary tftp://10.16.127.36/sys-vg-2
boot system rpm1 default tftp://10.16.127.35/sys-vg-2
boot system gateway 10.16.130.254
!
no logging console
!
hostname Dell
!
redundancy auto-failover-limit count 3 period 60
redundancy auto-synchronize full
!
enable password 7 b125455cf679b208fcf9eeeed0cd6d84
!
username admin password 7 1d28e9f33f99cf5c
!
linecard 0 provision C9000LC2410G
!
interface TenGigabitEthernet 0/0
 no ip address
 no shutdown
!
interface TenGigabitEthernet 0/1
 no ip address
 no shutdown
!
interface TenGigabitEthernet 0/2
 no shutdown
!
interface TenGigabitEthernet 0/3
 no ip address
 no shutdown
!
interface TenGigabitEthernet 0/4
 no ip address
 no shutdown
!
interface TenGigabitEthernet 0/5
 no shutdown
!
interface TenGigabitEthernet 0/6
 no ip address
 no shutdown
!
interface TenGigabitEthernet 0/7
 no ip address
 no shutdown
!
```

show running-config common

Use `show running-config common` to view the common configurations in the local system.

C9000 Series

Syntax `show running-config common`

Default None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the C9010.

Usage Information Use the `show running-config common` command to view only the common configurations in the local system.

Example

```
Dell#show running-config common
!
logging coredump
!
protocol lldp
!
feature extended-bridge
!
pe provision 10
 cascade interface TenGigabitEthernet 0/2
 cascade interface TenGigabitEthernet 0/2 peer
!
pe provision 11
 cascade interface TenGigabitEthernet 0/5
 cascade interface TenGigabitEthernet 0/5 peer
!
interface peGigE 255/0/1
 shutdown
!
--More--
```

show config

Display the configuration in the batch mode.

C9000 Series

Syntax `show config [common | user | local]`

Parameters

common	Displays the common configuration in the batch mode.
user	Displays the configuration done in the batch mode in an order entered by the user.
local	Displays the local configuration in the batch mode.

Command Modes CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the C9010.

Example

```
Dell(conf-b)#show config
interface vlan 10
interface vlan 20
no shutdown
interface vlan 30
interface vlan 40
ip access-list standard stdacl1
Dell(conf-b)#
```

```
Dell(conf-b)#show config user
interface vlan 10
exit
interface vlan 20
no shutdown
exit
interface vlan 30
exit
interface vlan 40
exit
ip access-list standard stdacl1
exit
```

write memory local

Use `write memory local` to save the local configurations to startup configuration.

C9000 Series

Syntax `write memory local`

Default None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced on the C9010.

Usage Information You can use the `write memory local` command to write only the local configurations to startup configuration.

Debugging

Use the commands in this section to debug the port extender hardware.

clear hardware system-flow pe

Clear the system-flow statistics from the specified port extender hardware component.

C9000 Series

Syntax

```
clear hardware system-flow pe pe-id stack-unit unit number port-set port-pipe-id counters
```

Parameters

pe *pe-id*	Enter the keyword `pe` and the port extender ID. Range is from 0 to 255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the stack unit number. Range is from 0 to 7.
port-set *port-pipe-id*	Enter the keyword `port-set` and the port pipe number. Port-pipe-id range is from 0 to 48.
counters	Enter the keyword `counters` to reset the system flow entry counter-values.

Defaults

None

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

Use the `clear hardware system-flow pe` command to clear the system flow statistics on a specified port extender and the stack unit in a PE stack.

Use the keywords `port-set` along with a port-pipe number, then the keyword counters to clear the system-flow counters on the selected port-pipe. The port-pipe value is 0.

Example

```
The example below is before and after clearing system-flow counters:

Dell#show hardware system-flow pe 255 stack-unit 1 port-set  0 counters
-------------------------------------------------------------------------
EntryId          Description                                    #HITS
-------------------------------------------------------------------------
1024        IPC traffic coming on PE Access Port           0
1023        IPC traffic destined to stack_unit 0 PE CPU    0
1022        IPC traffic destined to stack_unit 1 PE CPU    1011
1021        IPC traffic destined to stack_unit 2 PE CPU    12
1020        IPC traffic destined to stack_unit 3 PE CPU    0
1019        IPC traffic destined to stack_unit 4 PE CPU    0
1018        IPC traffic destined to stack_unit 5 PE CPU    0
1017        IPC traffic destined to stack_unit 6 PE CPU    0
1016        IPC traffic destined to stack_unit 7 PE CPU    0
1014        ECP traffic forwarded to next PE CPU           0
1013        ECP traffic destined to PE CPU                 139
1011        LLDP traffic forwarded to next PE CPU          36
1010        LLDP traffic destined to PE CPU                45
```

```
1009        LLDP/LACP traffic coming on access port-0      0
1008        LLDP/LACP traffic coming on access port-1      0
1007        LLDP/LACP traffic coming on access port-2      0
1006        LLDP/LACP traffic coming on access port-3      0
1005        LLDP/LACP traffic coming on access port-4      0
1004        LLDP/LACP traffic coming on access port-5      0
1003        LLDP/LACP traffic coming on access port-6      0
1002        LLDP/LACP traffic coming on access port-7      0
1001        LLDP/LACP traffic coming on access port-8      0
1000        LLDP/LACP traffic coming on access port-9      0
999         LLDP/LACP traffic coming on access port-10     0
998         LLDP/LACP traffic coming on access port-11     0
997         LLDP/LACP traffic coming on access port-12     0
996         LLDP/LACP traffic coming on access port-13     0
995         LLDP/LACP traffic coming on access port-14     0
994         LLDP/LACP traffic coming on access port-15     0
993         LLDP/LACP traffic coming on access port-16     0
992         LLDP/LACP traffic coming on access port-17     0
991         LLDP/LACP traffic coming on access port-18     0
990         LLDP/LACP traffic coming on access port-19     0
989         LLDP/LACP traffic coming on access port-20     0
988         LLDP/LACP traffic coming on access port-21     0
987         LLDP/LACP traffic coming on access port-22     0
986         LLDP/LACP traffic coming on access port-23     0
985         LLDP/LACP traffic coming on access port-24     0
984         LLDP/LACP traffic coming on access port-25     0
983         LLDP/LACP traffic coming on access port-26     0
982         LLDP/LACP traffic coming on access port-27     0
981         LLDP/LACP traffic coming on access port-28     0
980         LLDP/LACP traffic coming on access port-29     0
979         LLDP/LACP traffic coming on access port-30     0
978         LLDP/LACP traffic coming on access port-31     0
977         LLDP/LACP traffic coming on access port-32     0
976         LLDP/LACP traffic coming on access port-33     0
975         LLDP/LACP traffic coming on access port-34     0
974         LLDP/LACP traffic coming on access port-35     0
973         LLDP/LACP traffic coming on access port-36     139
```

show software pemgr

Display the port extender (PE) manager data.

C9000 Series

Syntax

`show software pemgr` *`pe-id`* `{ipc-stats [message type` *`0–FFFFF`* `| service–id` *`0-FFFF`* `]| pq-stats {High | Medium | Low}| reg-client}`

From a **PE console**, use `show software pemgr{ipc-stats [message type` *`0–FFFFF`* `| service–id` *`0–FFFF`* `]| pq-stats {High | Medium | Low}| reg-client}` to view the PE manager software information.

Parameters

pe *pe-id*	Enter the keyword `pe` and the port extender ID. Range is from 0 to 255.
ipc-stats	Enter the keyword `ipc-stats` to display inter-module communication statistics.
message type	(Optional) Enter the keyword option `message type` to display the data in *0–FFFF* message data format.

service-d	(Optional) Enter the keyword option `service-id` to display the statistics with a specified service or module ID.
pq-stats	Enter the keyword `pq-stats` to display a summary of priority queue (PQ) based statistics.
High	(Optional) Enter the keyword `High` to display the statistics for the high priority queue.
Medium	(Optional) Enter the keyword `Medium` to display the statistics for the medium priority queue.
Low	(Optional) Enter the keyword `Low` to display the statistics for the low priority queue.
reg-client	Enter the `reg-client` keyword to display the registered manager — agent / (client) information.

Defaults None

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010. and C1048P.

Usage Information The `show software pemgr` command is supported on a C1048P console.

Example: show software pemgr pe 0 ipc-stats

```
Dell#show software pemgr pe-id  1 ipc-stats
     IPC Message Based Statistics
    --------------------------
        Serivce Name : CLI                Service Id        : 0x10

MType           : 0x1771                  EndPoint          : CB

EnQCount        :            0 packets    DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks

        Serivce Name : SYSADMTSK          Service Id        : 0x21

MType           : 0x1c29                  EndPoint          : CB

EnQCount        :            8 packets    DeQCount          :            8
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              2 ticks    Max Q Proc Time   :              3
ticks
AVG Proc Time   :              2 ticks    Max Proc Time     :              3
ticks


        Serivce Name : PEMGR              Service Id        : 0x14e

MType           : 0x192                   EndPoint          : CB
```

```
EnQCount        :          38c packets    DeQCount          :          38c
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              1
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              1
ticks


        Serivce Name : PEMGR              Service Id        : 0x14e

MType           : 0xb9f2                  EndPoint          : CB

EnQCount        :          486 packets    DeQCount          :          486
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              3
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              3
ticks

        Serivce Name : IFMGR              Service Id        : 0x8a

MType           : 0x1771                  EndPoint          : CB

EnQCount        :            0 packets    DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks


        Serivce Name : IFMGR              Service Id        : 0x8a

MType           : 0x2a5c                  EndPoint          : CB

EnQCount        :            5 packets    DeQCount          :            5
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks


        Serivce Name : IFMGR              Service Id        : 0x8a

MType           : 0x2a3b                  EndPoint          : CB

EnQCount        :            0 packets    DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks


        Serivce Name : IFMGR              Service Id        : 0x8a

MType           : 0x2a3c                  EndPoint          : CB
```

```
EnQCount        :            0 packets    DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks


        Serivce Name : IFMGR              Service Id        : 0x8a

MType           : 0x2a3d                  EndPoint          : CB

EnQCount        :            0 packets    DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks


        Serivce Name : IFMGR              Service Id        : 0x8a

MType           : 0x2a32                  EndPoint          : CB

EnQCount        :            1 packets    DeQCount          :            1
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks


        Serivce Name : IFMGR              Service Id        : 0x8a

MType           : 0x2a44                  EndPoint          : CB

EnQCount        :            0 packets    DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks


        Serivce Name : IFMGR              Service Id        : 0x8a

MType           : 0x2a45                  EndPoint          : CB

EnQCount        :           11 packets    DeQCount          :           11
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              1
ticks


        Serivce Name : IFMGR              Service Id        : 0x8a
```

```
MType           : 0x2a4f                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : PEMGR            Service Id        : 0x14e

MType           : 0x1771                EndPoint          : CB

EnQCount        :            4 packets  DeQCount          :            4
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : CLI              Service Id        : 0x10

MType           : 0xb9f4                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : SYSADMTSK        Service Id        : 0x21

MType           : 0x1771                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : DIAGMGR          Service Id        : 0x1c

MType           : 0x1771                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : POEMGR           Service Id        : 0xfb
```

```
MType           : 0x12d0                EndPoint          : CB

EnQCount        :            1 packets  DeQCount          :            1
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks
```

Example: show software pemgr pe *pe-id* pq-stats

```
Dell#show software pemgr pe-id  1 pq-stats
     Priority Queue Based Statistics
    -------------------------------

End_Point  Priority    Enqueue count   Dequeue count   Outstanding count
                        Packets         Packets         Packets


PE         LOW                    0               0                  0

PE         MEDIUM               880             880                  0

PE         HIGH                 180             180                  0

CB         LOW                    0               0                  0

CB         MEDIUM              1146            1145                  1

CB         HIGH                 769             769                  0

Total messages Enqueued from CB End Point :1917 packets
Total messages Dequeued from CB End Point :1916 packets
Total messages Enqueued from PE End Point :1060 packets
Total messages Dequeued from PE End Point :1060 packets
```

Examples: show software pemgr pe *pe-id* reg-client

```
Dell#show software pemgr pe-id  1 reg-clients
     Manager - Agent Registration Status
    -----------------------------------

                                        Stack Unit
Service Name   Service Id   0   1   2   3   4   5   6   7

CHMGR                19   1   0   0   0   0   0   0   0

POEAGT               54   1   0   0   0   0   0   0   0

ACL                  57   1   0   0   0   0   0   0   0

ACL_AGENT            58   1   0   0   0   0   0   0   0

IFAGT                71   1   0   0   0   0   0   0   0

DIFFSERV             90   1   0   0   0   0   0   0   0

MACMGR               96   1   0   0   0   0   0   0   0

DSAGT               108   1   0   0   0   0   0   0   0

IFMGR               138   1   0   0   0   0   0   0   0

MRTM                139   1   0   0   0   0   0   0   0

L2AGENT             144   1   0   0   0   0   0   0   0

PORTMIRR            191   1   0   0   0   0   0   0   0
```

```
SFL_LP                194   1   0   0   0   0   0   0   0

SFL_CP                195   1   0   0   0   0   0   0   0

POEMGR                251   1   0   0   0   0   0   0   0
```

Example: show software pemgr pe 0 ipc-stats (PE Console)

```
Dell#show software pemgr ipc-stats
     IPC Message Based Statistics
    ----------------------------

        Serivce Name : CLI               Service Id        : 0x10

MType           : 0x1771                 EndPoint          : CB

EnQCount        :            0 packets   DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks   Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks   Max Proc Time     :              0
ticks


        Serivce Name : SYSADMTSK         Service Id        : 0x21

MType           : 0x1c29                 EndPoint          : CB

EnQCount        :            0 packets   DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks   Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks   Max Proc Time     :              0
ticks


        Serivce Name : PEMGR             Service Id        : 0x14e

MType           : 0x192                  EndPoint          : CB

EnQCount        :            0 packets   DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks   Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks   Max Proc Time     :              0
ticks


        Serivce Name : PEMGR             Service Id        : 0x14e

MType           : 0xb9f2                 EndPoint          : CB

EnQCount        :            0 packets   DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks   Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks   Max Proc Time     :              0
ticks


        Serivce Name : IFMGR             Service Id        : 0x8a
```

```
MType           : 0x1771                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : IFMGR            Service Id        : 0x8a

MType           : 0x2a5c                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : IFMGR            Service Id        : 0x8a

MType           : 0x2a3b                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : IFMGR            Service Id        : 0x8a

MType           : 0x2a3c                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : IFMGR            Service Id        : 0x8a

MType           : 0x2a3d                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : IFMGR            Service Id        : 0x8a
```

```
MType           : 0x2a32                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


                Serivce Name : PEMGR             Service Id        : 0x14e

MType           : 0x1771                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : CLI               Service Id        : 0x10

MType           : 0xb9f4                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : SYSADMTSK         Service Id        : 0x21

MType           : 0x1771                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks


        Serivce Name : DIAGMGR           Service Id        : 0x1c

MType           : 0x1771                EndPoint          : CB

EnQCount        :            0 packets  DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks  Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks  Max Proc Time     :              0
ticks
```

```
        Serivce Name : POEMGR             Service Id        : 0xfb

MType           : 0x12d0                  EndPoint          : CB

EnQCount        :            0 packets    DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks


        Serivce Name : POEMGR             Service Id        : 0xfb

MType           : 0x12ce                  EndPoint          : CB

EnQCount        :            0 packets    DeQCount          :            0
packets
Messages in Q   :            0 packets

AVG Q Proc Time :              0 ticks    Max Q Proc Time   :              0
ticks
AVG Proc Time   :              0 ticks    Max Proc Time     :              0
ticks


        Serivce Name : POEMGR             Service Id        : 0xfb

MType           : 0x12cf                  EndPoint          : CB
```

Example: show software pemgr pe-id 1 pq-stats (PE Console)

```
Dell#show software pemgr pe-id  1 pq-stats
     Priority Queue Based Statistics
    -------------------------------

End_Point   Priority    Enqueue count   Dequeue count   Outstanding count
                        Packets         Packets         Packets


PE          LOW                   0               0                   0

PE          MEDIUM              880             880                   0

PE          HIGH                180             180                   0

CB          LOW                   0               0                   0

CB          MEDIUM             1146            1145                   1

CB          HIGH                769             769                   0

Total messages Enqueued from CB End Point :1917 packets
Total messages Dequeued from CB End Point :1916 packets
Total messages Enqueued from PE End Point :1060 packets
Total messages Dequeued from PE End Point :1060 packets
```

Example: show software pemgr reg-clients (PE Console)

```
Dell#show software pemgr reg-clients
     Manager - Agent Registration Status
    ----------------------------------

                                        Stack Unit
Service Name    Service Id   0   1   2   3   4   5   6   7


CHMGR                   19   1   0   0   0   0   0   0   0

POEAGT                  54   1   0   0   0   0   0   0   0
```

```
ACL                    57   1   0   0   0   0   0   0   0
ACL_AGENT              58   1   0   0   0   0   0   0   0
IFAGT                  71   1   0   0   0   0   0   0   0
DIFFSERV               90   1   0   0   0   0   0   0   0
MACMGR                 96   1   0   0   0   0   0   0   0
DSAGT                 108   1   0   0   0   0   0   0   0
IFMGR                 138   1   0   0   0   0   0   0   0
MRTM                  139   1   0   0   0   0   0   0   0
L2AGENT               144   1   0   0   0   0   0   0   0
PORTMIRR              191   1   0   0   0   0   0   0   0
SFL_LP                194   1   0   0   0   0   0   0   0
SFL_CP                195   1   0   0   0   0   0   0   0
POEMGR                251   1   0   0   0   0   0   0   0
```

Power over Ethernet (PoE)

Use the commands in this section to configure the Power over Ethernet (PoE) feature on a C1048P port-extender (PE). PoE is not supported on C9010 switches. To manage PoE on port-extender ports, the C1048P uses two types of power supplies: the main internal, fixed AC power supply and an external DC power supply. Each power supply provides 1000W, of which up to 850W is used for PoE. For information about using the PoE stacking feature, refer to the "Power over Ethernet (PoE)" chapter in the Dell Networking OS Configuration Guide for the C9000 Series. The following PoE commands are supported on the Dell Networking OS.

advertise dot3-tlv

Configure the system or an interface to advertise IEEE 802.3at extended power-via-mdi.

C9000 Series

Syntax

`advertise dot3-tlv power-via-mdi`

To remove the advertised dot3–tlv, use the `no advertise dot3-tlv power-via-mdi` command

Parameters

power-via-mdi Enter the keyword `power–via-mdi` to advertise IEEE 802.3at power-via-mdi TLV.

Defaults

Disabled

Command Modes

- LLDP CONFIGURATION (conf-lldp)
- INTERFACE LLDP CONFIGURATION (conf-if-*interface*-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

The `advertise dot3-tlv power—via—mdi` command enables the system to advertise IEEE 802.3at power-via-mdi TLV to advertise its power negotiation capabilities with the powered devices via Link Layer Discovery Protocol (LLDP). You can configure this command either on a specific interface or globally.

Example

```
Dell(conf)#interface peGigE 0/0/0
Dell(conf-if-pegi-0/0/0)#protocol lldp
Dell(conf-if-pegi-0/0/0-lldp)#advertise dot3-tlv power-via-mdi
Dell(conf-if-pegi-0/0/0-lldp)#
```

advertise med power-via-mdi

Configure the system to advertise IEEE 802.1ab extended power-via— MDI TLV.

C9000 Series

Syntax

`[no] advertise med power-via-mdi`

To return to the default, use the `no advertise med power-via-mdi` command.

Parameters

power-via-mdi	Enter the keyword `power—via-mdi` to advertise IEEE 802.1ab MED Extended power-via-mdi TLV.

Defaults

Disabled

Command Modes

- LLDP CONFIGURATION (conf-lldp)
- INTERFACE LLDP CONFIGURATION (conf-if-*interface*-lldp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

Advertise extended power via MDI TLVs to all ports that are connected to the 802.1ab powered endpoint devices.

When the `advertise med power-via-mdi` command is enabled in CONFIGURATION mode, advertisement is enabled for all the interfaces in a system. To enable advertisement for a specific interface, configure the command in INTERFACE configuration mode.

Port extender (PE) processes and advertises LLDP power-via-MDI TLVs when the LLDP advertisement of the TLV is enabled on the PE in class power management mode. Incoming LLDP messages are processed only when the PE is in class power management mode.

on-disable

Enable transmission of LLDP shutdown frames.

C9000 Series

Syntax `on-disable transmit {shutdown}`

Parameters

transmit	Enter the keyword `transmit` to transmits the LLDP frames.
shutdown	Enter the keyword `shutdown` to shut down the LLDP frames.

Defaults None.

Command Modes CONFIGURATION INTERFACE (conf-if-*interface*-lldp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information The `on-disable transmit shutdown` command allows transmission of LLDP shutdown frames when the LLDP protocol is disabled in the interface mode.

Example

```
Dell#sh running-config interface tengigabitethernet 0/1
!
interface TenGigabitEthernet 10/1
 no ip address
 switchport
 switchport mode private-vlan host
!
 protocol lldp
on-disable  transmit shutdown
 no shutdown
```

Related Commands show running-config lldp — displays the LLDP running configuration.

power budget global-threshold

Set a global threshold limit for the PoE power budget on a specified port extender.

C9000 Series

Syntax `power budget global-threshold pe pe-id stack-unit unit number threshold-value`

Parameters

pe *pe-id*	Enter the keyword `pe` and port extender ID. Range is from 0 to 255.
stack-unit *unit number*	Enter the keyword `stack-unit` and unit number. Range is from 0 to 7.
threshold-value	Enter the power threshold limit value in percentage. Range is from 10 to 99%. Default value is 99%.

Default None

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.

Usage Information Configure a global threshold limit for the Power over Ethernet (PoE) power budget for a specified port extender. A default power threshold value of 99% is configured when there is no threshold value configured.

Use this command in Configuration Terminal Batch mode to configure the threshold limit for the PoE power budget in a dual-homing setup.

Example

```
Dell(conf)#power budget global-threshold pe 1 stack-unit 0 99

Dell#show power detail pe 0 stack-unit 0
Unit    Total      System   Redundancy Inline     Inline    Inline    Inline   Inline
        Power      Power    Power      Power      Power     Power     Power    Power
        Available  Consumed Consumed   Threshold  Available Allocated Consumed Remaining
        (Watts)    (Watts)  (Watts)    (%)        (Watts)   (Watts)   (Watts)  (Watts)
--------- ---------- --------- --------- --------- --------- --------- --------------
0/0     1000        150          0        99       841        0          0      841
```

Related Command show power detail

power inline

Enable inline power and configure maximum power allocation with priority for the powered device connected to an interface.

C9000 Series

Syntax

```
power inline {[max_milliwatts ]| priority {critical | high | low}}
```

To disable a device that has been enabled for PoE power supply, use the `no power inline` command.

Parameters

max_milliwatts	(OPTIONAL) Specify the maximum amount of inline power allocation to a powered device connected to the interface. Range is 440–30000 milliwatts (mWs). The default value is 30000 mWs. **NOTE: The *max_milliwatt* configuration is effective only in Static mode.**
priority	Enter the keyword `priority` to specify the PoE priority for the powered device connected to the interface. Default priority value is low.
critical	Enter the keyword `critical` to set the PoE priority level as critical.
high	Enter the keyword `high` to set the PoE priority level as high.
low	Enter the keyword`low` to set the PoE priority as low.

Defaults

Default priority is low.

Command Modes

INTERFACE CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage information

The `power inline [max_milliwatts}` command enables inline power supply to an interface. You can specify the maximum amount of power allocation to a device in max-milliwatts, within a range of 440–30000 mW. If a specific power supply value is not configured, the default value of 30,000 mW is configured as the maximum power for allocation to powered devices. You can disable the inline power supply to a port using the `no power inline` command.

The `power inline priority` command allows you to specify the power inline priority for an interface when a power shortage occurs. PoE is removed from ports configured with `low` priority first, then ports configured with `high` priority are disabled. The ports configured with `critical` priority are the last ports disabled during a power shortage. When two or more ports are configured with same priority level, the ports with higher interface numbers are disabled first. For example, if ports 1, 2, 47, and 48 are all configured with a `low` priority and there is a shortage of inline power supply, PoE is first disabled on port 48, followed by port 47 and, then port 2. Port 1 (with the lowest interface number) takes precedence over all other ports and is disabled after all other ports are disabled.

Example

```
Dell(conf)#int peGigE 0/0/0
Dell(conf-if-pegi-0/0/0)#power inline 30000
Dell(conf-if-pegi-0/0/0)#power inline priority critical

Dell(conf-if-pegi-0/0/0)#  Dell#show power inline pe 0 stack-unit 0
Global inline power Threshold         : 99
Power Reserved for inline Power        : 841W
Total Inline Power Consumed        : 0W
Remaining inline power Available    : 841W
Power Management Mode            : Static

Interface       Inline Power   Inline Power    Class   Device   PoE Port
LLDP
                Max / Alloc     Consumed                Type    Priority
Support
                (Watts)        (Watts)
-------------   ------------   ------------   -------  ------   --------
------
PeGi 0/0/0       30.00/0.00         0.00       NO_PD      -     critical
0
```

power inline legacy

Allocate inline power to the legacy devices on a Port Extender .

C9000 Series

Syntax

`power inline legacy {pe` *`pe-id`* `stack-unit` *`unit number`*`}`

To disable the detection of legacy powered devices in a port extender, use the `no power inline legacy {pe` *`pe-id`* `stack-unit` *`unit number`*`}` command.

Parameters

pe *pe-id*	Enter the keyword `pe` and the port extender ID. Range is 0–255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the unit number. Range is 0–7.

Defaults

Enabled

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.

Usage Information

The `power inline legacy` command allows the system to detect and allocate inline power to the legacy devices on a Port Extender.

Use this command in Configuration Terminal Batch mode to allocate inline power to the legacy devices in a dual-homing setup.

Example

```
Dell(conf)#power inline legacy pe 0 stack-unit 0
```

power inline mode

Configures PoE power management mode for a specified port extender.

C9000 Series

Syntax

```
power inline mode {pe pe-id stack-unit unit number class | static }
```

Parameters

pe *pe-id*	Enter the keyword `pe` and port extender ID. Range is 0–255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the unit number. Range is 0–7.
class	Enter the keyword `class` to configure the class mode for the specified port extender.
static	Enter the keyword `static` to configure the static mode for the specified port extender.

Defaults

Static

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.

Usage Information

The `power inline mode` command allows you to manage inline power supply on the port extender (PE) ports. You can configure `class` or `static` mode to manage inline power in a port extender.

When `class` mode is configured, maximum power for the particular class of device is allocated. Class mode supports power allocation via Layer 2 classification and power negotiation by Link Layer Discovery Protocol (LLDP) 802.3at standard . When `static` mode is configured, the inline power is allocated based on the actual power consumption by the powered device. Power negotiation via LLDP is not supported in `static` mode.

Use this command in Configuration Terminal Batch mode to manage inline power supply in a dual-homing setup.

The following examples show power management mode, “class” configured for the port extender 255.

Example

```
Dell(conf)#power inline mode pe 0 stack-unit 0 static

Dell#show power inline pe 0 stack-unit 0

Global inline power Threshold :           99
Power Reserved for inline Power:          841W
Total Inline Power Consumed:              0W
Remaining inline power Available:         841W
Power Management Mode:                    Static

Interface       Inline Power   Inline Power    Class   Device   PoE Port
LLDP
                Max / Alloc     Consumed                Type    Priority
Support
                (Watts)        (Watts)
-------------   ------------   ------------   -------  ------   --------
------
PeGi 0/0/0     30.00/0.00       0.00           NO_PD      -      low
0
```

power inline restore pe

Enable the temporarily suspended PoE power supply to all the ports in a port extender unit.

C9000 Series

Syntax `power inline restore pe` *`pe-id`* `stack-unit` *`unit number`*

Parameters

pe *pe-id*	Enter the keyword `pe` and the port extender ID. Range is from 0 to 255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the stack-unit number. Range is from 0 to 7.

Defaults None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information The `power inline restore pe` command enables or restores the temporarily suspended PoE power supply to all the ports on a port extender unit.

Example

```
Dell#power inline restore pe 1 stack-unit 2
```

power inline suspend pe

Disable PoE power supply to all the ports in a port extender unit temporarily.

C9000 Series

Syntax `power inline suspend pe pe-id stack-unit unit number`

Parameters

pe *pe-id*	Enter the keyword `pe` and the port extender ID. Range is 0–255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the stack unit number. Range is 0–7.

Defaults None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information The `power inline suspend pe` command temporarily disables PoE power supply to all the ports in a port extender (PE) unit. You can use the `power inline restore pe` command to restore or enable the PoE power supply to the PE unit.

Example

```
Dell#power inline suspend pe 1 stack-unit 2
% Error: StackUnit 2 of PE 1 not provisioned/connected
```

upgrade poe-controller

Manually upgrade the PoE controller firmware for a specified port extender unit.

C9000 Series

Syntax `upgrade poe-controller pe pe-id stack-unit unit number`

Parameters

pe *pe-id*	Enter the keyword `pe` and port extender ID. Range is from 0 to 255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the unit number. Range is from 0 to 7.

Defaults None

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

The `upgrade poe-controller pe` command is used to manually upgrade the PoE controller firmware for a specified port extender unit.

You can upgrade the PoE controller firmware using the firmware image that is packed with the Dell Networking OS. Once the upgrade is successful, the Port Extender reloads automatically.

In a dual homing setup, you can use this command only from the primary VLT peer.

Example

```
Dell#upgrade poe-controller pe 254 stack-unit 1
```

show power inline

Display the PoE power allocation on a specified port extender.

C9000 Series

Syntax

```
show power inline {pe pe-id stack-unit unit number | interface interface }
```

Parameters

pe *pe-id*	Enter the keyword `pe` and the port extender ID. Range is from 0 to 255.
stack-unit *unit number*	Enter the keyword `stack-unit` and the stack unit number Range is from 0 to 7.
interface *interface*	Enter the `interface` keyword, and specify one of the following *interface* types: • For a PE Gigabit Ethernet interface, enter the keyword `peGigE`. You must specify a *pe-id/Unit/Port* for the interface. • For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults

None

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.

Usage Information

The following describes the output fields of the `show power inline` command:

Field	Description
Interface	Displays the line card or the port extender interface slot and port number.
Inline Power Allocated	Displays the amount of power allocated to the port.
Inline Power Consumed	Displays the amount of power consumed by the connected device.
Class	Displays the power classification of the connected device. If the device is powered up properly, it displays Class 0, 1, 2, 3, or 4. Displays the following under different conditions: • NO_DEVICE if no device is present. • LEGACY if a legacy device is connected. • PD_S/C if a short-circuit condition is detected. • PD_OVRLD if overload condition is detected.
Device Type	Displays whether the device is Type 1 or Type 2.
PoE Port Priority	Displays the power configured for the port (default is low). See `power inline priority`.
LLDP Support	Displays the power requested is via LLDP-MED extended power-via-mdi TLV or IEEE 802.3at power-via-mdi TLV.

Example

```
Dell#show power inline pe 255 stack-unit 0



Global inline power Threshold :           99
Power Reserved for inline Power:          1612W
Total Inline Power Consumed:              21W
Remaining inline power Available:         1580W
Power Management Mode:                    Class

Interface       Inline Power   Inline Power    Class   Device   PoE Port
LLDP
                Max / Alloc     Consumed                Type    Priority
Support
                (Watts)         (Watts)
--------------   ------------   ------------   -------  ------   --------
------
PeGi 255/0/0     30.00/21.40       21.50         4        2      low
0
```

show power detail

Display the inline power consumption details for a port extender.

C9000 Series

Syntax `show power detail {pe pe-id stack-unit unit number}`

Parameters

pe	Enter the keyword `pe` and the port externder ID. Range is 0–255.
stack-unit	Enter the `stack-unit` keyword and the unit ID. Range is 0–7.

Defaults None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Example

```
Dell#show power detail pe 2 stack-unit 1

Unit Total  System Redundancy  Inline  Inline  Inline  Inline  Inline
         Power  Power  Power       Power   Power   Power   Power   Power
     Available Consumed Consumed   Threshold Available Allocated Consumed
Remaining
      (Watts)  (Watts)  (Watts)     (%)       (Watts) (Watts) (Watts) (Watts)
-----------------------------------------------------------------------------------------------------------
2/1    2000.00   150      150       90       1530.00  308.00  190.00  1222.00
```

show revision

View the PoE controller firmware version running on the port extender.

C9000 Series

Syntax `show revision {pe pe-id stack-unit unit number}`

From a **PE console**, use `show revision` to view the revision levels.

Parameters

pe *pe-id*	Enter the keyword `pe` and the port extender ID. Range is from 0 to 255.
stack-unit *unit-number*	Enter the keyword `stack-unit` and the unit number. Range is from 0 to 7.

Defaults None

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.

Example

```
Dell#show revision pe 0

DEVICE IMAGE INFORMATION :
-------------------------------------------------------
     Type            Version        Target
     FPGA             3.7            LP (0)
     CPLD             3.0            LP (0)
     IAP              3.1            LP (0)
     FPGA             3.7            LP (1)
     CPLD             3.0            LP (1)
     IAP              3.1            LP (1)
     FPGA             3.7            LP (2)
     CPLD             3.0            LP (2)
     IAP              3.1            LP (2)
     FPGA             3.7            LP (3)
     CPLD             3.0            LP (3)
     IAP              3.1            LP (3)
     FPGA             3.7            LP (4)
     CPLD             3.0            LP (4)
     IAP              3.1            LP (4)
     FPGA             3.7            LP (5)
     CPLD             3.0            LP (5)
     IAP              3.1            LP (5)
     FPGA             3.7            LP (6)
     CPLD             3.0            LP (6)
     IAP              3.1            LP (6)
     FPGA             3.7            LP (7)
     CPLD             3.0            LP (7)
     IAP              3.1            LP (7)
     FPGA             3.7            LP (8)
     CPLD             3.0            LP (8)
     IAP              3.1            LP (8)
     FPGA 1           3.9            CP
     CPLD             3.5            CP
     FPGA 2           2.0            CP
     Backup FPGA      2.0            CP
     IAP              3.1            CP
     CPLD             16             pe (0/0)
     Boot Flash       3.3.1.7        pe (0/0)
     CPLD             16             pe (1/0)
     Boot Flash       3.3.1.7        pe (1/0)
     CPLD             16             pe (2/0)
     Boot Flash       3.3.1.7        pe (2/0)
     CPLD             16             pe (4/0)
     Boot Flash       3.3.1.7        pe (4/0)
     CPLD             13             pe (6/100)
     Boot Flash                      pe (6/100)
```

Exmaple (PE Console)

```
Dell#show revision

--  Stack unit 1  --
CPLD                   : 13
```

47

Port Monitoring

The port monitoring feature allows you to monitor network traffic by forwarding a copy of each incoming or outgoing packet from one port to another port.

Important Points to Remember

- Port monitoring is supported on physical ports and logical interfaces, such as port channels and virtual local area networks (VLANs).
- The monitoring (destination, "MG") and monitored (source, "MD") ports must be on the same switch.
- In general, a monitoring port should have `no ip address` and `no shutdown` as the only configuration; Dell Networking OS permits a limited set of commands for monitoring ports; display them using the `?` command. A monitoring port also may not be a member of a VLAN.
- A total of 4 MG may be configured in a single port-pipe.
- MG and MD ports can be reside anywhere across a port-pipe.
- The Dell Networking OS supports multiple source ports to be monitored by a single destination port in one monitor session.
- One monitor session can have only one MG port.
- PE Gigabit Ethernet (peGigE) ports can be added as source ports only. You cannot add cascade ports as destination ports.

NOTE: The monitoring port should not be a part of any other configuration.

Topics:

- description
- erpm
- monitor session
- show config
- show monitor session
- show running-config monitor session
- source (port monitoring)

description

Enter a description of this monitoring session.

C9000 Series

Syntax `description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description regarding this session (80 characters maximum).

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.7.1.0	Introduced on the E-Series.

Related Commands monitor session — enables a monitoring session.

erpm

Configure the source and destination IP address for ERPM traffic.

Syntax `erpm source-ip` *`ip-address`* `dest-ip` *`ip-address`* `[gre-protocol` *`value`*`]`

To remove the configuration, use the `no erpm source-ip` *`IP-address`* `dest-ip` *`IP-address`* `[gre-protocol` *`value`*`]` command.

Parameters

source–ip *ip-address*	Enter the keywords `source-ip` then the source IP address in dotted decimal format.
destination–ip *ip-address*	Enter the keywords `dest-ip` then the destination IP address in dotted decimal format.
gre–protocol *value*	(OPTIONAL) Enter the keywords `gre-protocol` then the protocol type value for ERPM type monitor session. The range is from 1 to 65535.

Command Modes MONITOR SESSION (conf-mon- *sess-session-ID*)

Example

```
Dell(conf-mon-sess-10)#erpm source-ip 10.10.10.1 dest-ip 5.1.1.2 gre-protocol
1111
```

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Introduced GRE protocol support.

monitor session

Create a session for monitoring traffic with port monitoring.

C9000 Series

Syntax

`monitor session` *`session-ID`* `(type { rpm | erpm })`

To delete a session, use the `no monitor session` *`session-ID`* command.

To delete all monitor sessions, use the `no monitor session all` command.

Parameters

session-ID	Enter a session identification number. The range is from 0 to 65535.
type rpm | erpm	Specifies one of the following type: • `rpm`: to create remote port monitoring session. • `erpm`: to create encapsulated remote port monitoring session.

Defaults

none

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.
9.0.2.0	Introduced on the S6000.
9.0.2.0	Introduced on the MXL.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information

The `monitor` command is saved in the running configuration at Monitor Session mode level and can be restored after a chassis reload.

Use this command in Configuration Terminal Batch mode to monitor the traffic in a dual-homing setup.

Example

```
Dell(conf)# monitor session 60
Dell(conf-mon-sess-60)
```

Related Command

show monitor session — displays the monitor session.

show running-config monitor session — displays the running configuration of a monitor session.

show config

Display the current monitor session configuration.

C9000 Series

Syntax

```
show config
```

Defaults

none

Command Modes

MONITOR SESSION (conf-mon-*sess-session-ID*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell(conf-mon-sess-2)#show config
!
monitor session 2 type rpm
 source fortyGigE 0/60 destination remote-vlan 300 direction rx
 source Port-channel 10 destination remote-vlan 300 direction rx
 no disable
Dell#
```

show monitor session

Display port extender (PE) Gigabit Ethernet interface monitoring information.

C9000 Series

Syntax

`show monitor session {session-ID}`

To display monitoring information for all sessions, use the `show monitor session` command.

To display monitoring information for port extender interface, when added as a source port, use the `do show monitor session` command in CONFIGURATION mode.

Parameters

session-ID (OPTIONAL) Enter a session identification number. The range is from 0 to 65535.

Defaults

none

Command Modes

- CONFIGURATION
- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Introduced the support for GRE Protocol and FC Monitor in the command output.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4.0.0	Added support for the RPM / ERPM.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Example

```
Dell#show monitor session 1
SessID Source   Destination Dir Mode SourceIP DestIP  DSCP TTL Drop Rate  Gre-Protocol
FcMonitor
-----  ------   ----------- --- ---- -------- ------- ---- --- ---  ----  ------------
---------
```

```
  1  PeGi 0/0/0  Te 10/2     rx Port  0.0.0.0 0.0.0.0 0   0   0  No   N/A      N/
A           Yes
```

Related Commands monitor session — creates a monitoring session.

show running-config monitor session

Display the running configuration of all monitor sessions or a specific session.

C9000 Series

Syntax `show running-config monitor session {session-ID}`

To display the running configuration for all monitor sessions, use the `show running-config monitor session` command.

Parameters

session-ID	(OPTIONAL) Enter a session identification number. The range from 0 to 65535.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information The `monitoring` command is saved in the running configuration at the Monitor Session mode level and can be restored after a chassis reload.

Example

```
Dell(conf-mon-sess-0)#do show running-config monitor session
!
monitor session 0
```

```
 source Port-channel 10 destination TenGigabitEthernet 0/33 direction tx
!
```

Related Commands

monitor session — creates a monitoring session.

show monitor session — displays a monitoring session.

source (port monitoring)

Configure a port monitor source.

C9000 Series

Syntax

`source interface | range destination interface direction {rx | tx | both}`

To disable a monitor source, use the `no source interface destination interface direction {rx | tx | both}` command.

Parameters

source *interface*

Enter the one of the following keywords and slot/port information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port channel interface, enter the keyword `port-channel` and a port-channel ID.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.
- For a VLAN interface, enter the keyword `VLAN` and a *vlan-id* number. Range is from 1 to 4094.
- For a remote VLAN interface, enter the keyword `Remote-VLAN` and a *vlan-id* number. Range is from 1 to 4094
- For a port channel interface, enter the keyword `port-channel` and a port-channel ID.

NOTE: You cannot configure VLAN 4092 and 4093. These VLANs are reserved for internal use.

range

Enter the keyword `range` to specify the list of interfaces.

destination

Enter the keyword `destination` to specify the destination interface.

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

- For a port channel interface, enter the keyword `port-channel` and a the port-channel ID.
- For a remote VLAN interface, enter the keyword `Remote-VLAN` and a *vlan-id* number. Range is from 1 to 4094

interface Enter the one of the following keywords and slot/port information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN interface, enter the keyword `VLAN` and a *vlan-id* number. Range is from 1 to 4094.
- For a port channel interface, enter the keyword `port-channel` amd a the port-channel ID.

direction {rx | tx | both} Enter the keyword `direction` then one of the packet directional indicators.

- `rx`: to monitor receiving packets only.
- `tx`: to monitor transmitting packets only.
- `both`: to monitor both transmitting and receiving packets.

Defaults none

Command Modes MONITOR SESSION (conf-mon- *sess-session-ID*)

Command History This guide is platform-specific. For command information about other platforms, see to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4.0.0	Added support for Source and destination.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

You can configure a port extender (PE) Gigabit Ethernet `peGigE` port as a source port in the `source (port monitoring)` command and monitor traffic flow on this port. You cannot configure a cascade port as a destination port.

Example

```
Dell# monitor session 0
source Port-channel 10 destination TenGigabitEthernet 0/33 direction tx
```

48

Private VLAN (PVLAN)

The private VLAN (PVLAN) feature of the Dell Networking operating software.

Private VLANs extend the system security suite by providing Layer 2 isolation between ports within the same private VLAN. A private VLAN partitions a traditional VLAN into subdomains identified by a primary and secondary VLAN pair. The private VLAN implementation is based on RFC 3069.

For more information, see the following commands. The command output is augmented in the Dell Networking OS version 7.8.1.0 at later to provide PVLAN data:

- show arp
- show vlan

Private VLAN Concepts

Primary VLAN:

The primary VLAN is the base VLAN and can have multiple secondary VLANs. There are two types of secondary VLAN — community VLAN and isolated VLAN:

- A primary VLAN can have any number of community VLANs and isolated VLANs.
- Private VLANs block all traffic to isolated ports except traffic from promiscuous ports. Traffic received from an isolated port is forwarded only to promiscuous ports or trunk ports.

Community VLAN:

A community VLAN is a secondary VLAN of the primary VLAN:

- Ports in a community VLAN can talk to each other. Also, all ports in a community VLAN can talk to all promiscuous ports in the primary VLAN and vice versa.
- Devices on a community VLAN can communicate with each other using member ports, while devices in an isolated VLAN cannot.

Isolated VLAN:

An isolated VLAN is a secondary VLAN of the primary VLAN:

- Ports in an isolated VLAN cannot talk to each other. Servers would be mostly connected to isolated VLAN ports.
- Isolated ports can talk to promiscuous ports in the primary VLAN, and vice versa.

Port Types:

- *Community port*: A community port is a port that belongs to a community VLAN and is allowed to communicate with other ports in the same community VLAN and with promiscuous ports.
- *Isolated port*: An isolated port is a port that, in Layer 2, can only communicate with promiscuous ports that are in the same PVLAN.
- *Promiscuous port*: A promiscuous port is a port that is allowed to communicate with any other port type.
- *Trunk port*: A trunk port carries VLAN traffic across switches:
  - A trunk port in a PVLAN is always tagged.
  - A trunk port in Tagged mode carries primary or secondary VLAN traffic. The tag on the packet helps identify the VLAN to which the packet belongs.

– A trunk port can also belong to a regular VLAN (non-private VLAN).

Topics:

- ip local-proxy-arp
- private-vlan mode
- private-vlan mapping secondary-vlan
- show interfaces private-vlan
- show vlan private-vlan
- switchport mode private-vlan

ip local-proxy-arp

Enable/disable Layer 3 communication between secondary VLANs in a private VLAN.

C9000 Series

Syntax

`[no] ip local-proxy-arp`

To disable Layer 3 communication between secondary VLANs in a private VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the primary VLAN.

To disable Layer 3 communication in a particular secondary VLAN, use the `no ip local-proxy-arp` command in INTERFACE VLAN mode for the selected secondary VLAN.

NOTE: Even after you disable `ip-local-proxy-arp` in a secondary VLAN, Layer 3 communication may happen between some secondary VLAN hosts, until the ARP timeout happens on those hosts.

Defaults

Layer 3 communication is disabled between secondary VLANs in a private VLAN.

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Related Commands

- private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary.
- private-vlan mapping secondary-vlan — maps secondary VLANs to the selected primary VLAN.
- show arp — displays the ARP table.
- show interfaces private-vlan — displays the type and status of the PVLAN interfaces.

- show vlan private-vlan — displays the PVLANs and/or interfaces that are part of a PVLAN.
- switchport mode private-vlan — sets PVLAN mode of the selected port.

private-vlan mode

Set PVLAN mode of the selected VLAN to community, isolated, or primary.

C9000 Series

Syntax

`[no] private-vlan mode {community | isolated | primary}`

To remove the PVLAN configuration, use the `no private-vlan mode {community | isolated | primary}` command syntax.

Parameters

community	Enter the keyword `community` to set the VLAN as a community VLAN.
isolated	Enter the keyword `isolated` to configure the VLAN as an isolated VLAN.
primary	Enter the keyword `primary` to configure the VLAN as a primary VLAN.

Defaults

none

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

The VLAN:

- can be in only one mode, either `community`, `isolated`, or `primary`.
- mode ode to `community` or `isolated` even before associating it to a primary VLAN. This secondary VLAN continues to work normally as a normal VLAN even though it is not associated to a primary VLAN. (A syslog message shows this information.)
- must not have a port in it when VLAN mode is being set.

Only ports (and port channels) configured as promiscuous, host, or PVLAN trunk ports (as previously described) can be added to the PVLAN. No other regular ports can be added to the PVLAN.

After using this command to configure a VLAN as a primary VLAN, use the `private-vlan mapping secondary-vlan` command to map secondary VLANs to this VLAN.

Related Commands

- private-vlan mapping secondary-vlan — maps secondary VLANs to the selected primary VLAN.
- show interfaces private-vlan — displays the type and status of the PVLAN interfaces.
- show vlan private-vlan — displays the PVLANs and/or interfaces that are part of a PVLAN.
- switchport mode private-vlan — sets PVLAN mode of the selected port.

private-vlan mapping secondary-vlan

Map secondary VLANs to the selected primary VLAN.

C9000 Series

Syntax

`[no] private-vlan mapping secondary-vlan vlan-list`

To remove specific secondary VLANs from the configuration, use the `no private-vlan mapping secondary-vlan vlan-list` command syntax.

Parameters

vlan-list	Enter the list of secondary VLANs to associate with the selected primary VLAN. The list can be in comma-delimited or hyphenated-range format, following the convention for the range input.

Defaults

none

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

The list of secondary VLANs can be:

- Specified in comma-delimited or hyphenated-range format.
- Specified with this command even before they have been created.
- Amended by specifying the new secondary VLAN to be added to the list.

Related Commands

- private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary.
- show interfaces private-vlan — displays the type and status of the PVLAN interfaces.
- show vlan private-vlan — displays the PVLANs and/or interfaces that are part of a PVLAN.
- switchport mode private-vlan — sets PVLAN mode of the selected port.

show interfaces private-vlan

Display type and status of PVLAN interfaces.

C9000 Series

Syntax `show interfaces private-vlan [interface interface]`

Parameters

interface *interface* (OPTIONAL) Enter the keyword `interface` and the interface type, slot/port numbers or port-channel number to specify the port(s) for which you want to display PVLAN information. Enter only a slot ID to display the PVLAN status for all ports on a line card. The valid values are:

- For a port channel interface, enter the keyword `port-channel` and a port-channel ID.
- For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

This command has two types of display — a list of all PVLAN interfaces or for a specific interface. Examples of both types of output are shown below.

The following describes the `show interfaces private-vlan` command shown in the examples below.

Field	Description
Interface	Displays the type of interface and associated slot and port number.
Vlan	Displays the VLAN ID of the designated interface.
PVLAN-Type	Displays the type of VLAN in which the designated interface resides.
Interface Type	Displays the PVLAN port type of the designated interface.
Status	States whether the interface is operationally up or down.

Example (All)

```
Dell# show interfaces private-vlan
 Interface Vlan PVLAN-Type Interface Type Status
 --------- ---- ---------- -------------- --------
 Fo 1/52   30   Isolated   Host           Up
 Fo 2/12   20   Community  Host           Up
 Po 10     10   Primary    Trunk          Up
```

Example (Specific)

```
Dell# show interfaces private-vlan te 2/2
Interface Vlan PVLAN-Type Interface Type Status
--------- ---- ---------- -------------- --------
Te 2/2    100  Isolated   Host           Up
```

Related Commands

- private-vlan mode – sets the mode of the selected VLAN to community, isolated, or primary.
- show vlan private-vlan – displays the PVLANs and/or interfaces that are part of a PVLAN.
- switchport mode private-vlan – sets PVLAN mode of the selected port.

show vlan private-vlan

Display PVLAN configurations, including member interfaces, type, and status.

C9000 Series

Syntax

```
show vlan private-vlan [vlan-id | community vlan-id | interface interface |
isolated vlan-id | mapping vlan-id | primary vlan-id]
```

Parameters

vlan-id	(OPTIONAL) Enter a VLAN ID number to display the PVLAN configuration.
community *vlan-id*	(OPTIONAL) Enter the keyword `community` and a PVLAN ID number to display the configuration for a community PVLAN.

interface *interface* (OPTIONAL) Enter the keyword `interface` and specify the interface type and slot/port numbers or port-channel number to display the PVLAN configuration for a member interface. The valid values are:

- For a port channel interface, enter the keyword `port-channel` and a port-channel ID.
- For a 10-Gigabit Ethernet interface, enter the keyword `tenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

isolated (OPTIONAL) Enter the keyword `isolated` and a PVLAN ID number to display the configuration of an isolated PVLAN.

mapping (OPTIONAL) Enter the keyword `mapping` to display the community and isolated PVLAN mapping to primary PVLANs.

primary *vlan-id* (OPTIONAL) Enter the keyword `primary` and a PVLAN ID number to display the configuration of a primary PVLAN.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

Examples of all types of command output are shown below. The first type of output is the result of not entering an optional keyword. It displays a detailed list of all PVLANs and their member VLANs and interfaces. The other types of output show details about PVLAN subsets.

The following describes the `show private-vlan` command shown in the Examples below.

Field	Description
Primary	Displays the VLAN ID of the designated or associated primary VLAN(s).
Secondary	Displays the VLAN ID of the designated or associated secondary VLAN(s).
Type	Displays the type of VLAN in which the listed interfaces reside.
Active	States whether the interface is operationally up or down.
Ports	Displays the interface IDs in the listed VLAN.

Example (All)

```
Dell# show vlan private-vlan
Primary Secondary Type      Active Ports
------- --------- --------- ------ -----------
10                primary   Yes    Te 2/1,3
        100       isolated  Yes    Te 2/2
        101       community Yes    Te 2/10
20                primary   Yes    Po 10, 12-13
                                   Te 1/1
        200       isolated  Yes    Te 1/2,4-6
        201       community No
        202       community Yes    Te 1/11-12
```

Example (Primary)

```
Dell# show vlan private-vlan primary
Primary Secondary Type    Active  Ports
------- --------- --------- ------ -------
10                primary  Yes    Te 2/1,3
20                primary  Yes    Te 1/1,3
```

Example (Isolated)

```
Dell# show vlan private-vlan isolated
Primary Secondary Type      Active Ports
------- --------- --------- ------ ----------
10                primary   Yes    Te 2/1,3
        100       isolated  Yes    Te 2/2,4-6
        200       isolated  Yes    Te 1/2,4-6
```

Example (Community)

```
Dell# show vlan private-vlan community
Primary Secondary Type      Active Ports
------- --------- --------- ------ -----------
10                primary   Yes    Te 2/1,3
        101       community Yes    Te 2/7-10
20                primary   Yes    Po 10, 12-13
                                   Te 1/1
        201       community No
        202       community Yes    Te 1/11-12
```

Example (Interface)

```
Dell# show vlan private-vlan interface te 2/1
Primary Secondary Type     Active Ports
------- --------- --------- --------------------
10                primary  Yes    Te 2/1
```

Example (Mapping)

```
Dell# show vlan private-vlan mapping

Private Vlan:
 Primary   : 10
 Isolated  : 30
 Community : 20
```

Usage Information

Note that if the VLAN ID you enter is a primary VLAN, the entire private VLAN output is displayed, as shown below. If the VLAN ID is a secondary VLAN, only its primary VLAN and secondary VLAN properties are displayed, as shown in the second Example below.

Example

```
Dell# show vlan private-vlan 10
Primary Secondary Type      Active  Ports
------- --------- --------- -------------------
10                primary   Yes     Te 2/1,3
        102       isolated  Yes     Te 0/4
        101       community Yes     Te 2/7-10
```

Example

```
Dell#show vlan private-vlan 102
Primary Secondary Type     Active Ports
------- --------- --------- --------------------
10                Primary   Yes    Po 1
                                   Te 0/2
        102       Isolated  Yes    Te 0/4
```

Related Commands

private-vlan mode – sets the mode of the selected VLAN to community, isolated, or primary.

show interfaces private-vlan – displays type and status of PVLAN interfaces.

switchport mode private-vlan – sets PVLAN mode of the selected port.

switchport mode private-vlan

Set PVLAN mode of the selected port.

C9000 Series

Syntax

`[no] switchport mode private-vlan {host | promiscuous | trunk}`

To remove PVLAN mode from the selected port, use the `no switchport mode private-vlan` command.

Parameters

host	Enter the keyword `host` to configure the selected port or port channel as an isolated interface in a PVLAN.
promiscuous	Enter the keyword `promiscuous` to configure the selected port or port channel as a promiscuous interface.
trunk	Enter the keyword `trunk` to configure the selected port or port channel as a trunk port in a PVLAN.

Defaults

Disabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information

The assignment of the various PVLAN port types to port and port channel (LAG) interfaces is shown in the following example.

Example

```
Dell#conf
Dell(conf)#interface TenGigabitEthernet 2/1
Dell(conf-if-te-2/1)#switchport mode private-vlan promiscuous

Dell(conf)#interface TenGigabitEthernet 2/2
Dell(conf-if-te-2/2)#switchport mode private-vlan host

Dell(conf)#interface TenGigabitEthernet 2/3
Dell(conf-if-te-2/3)#switchport mode private-vlan trunk

Dell(conf)#interface port-channel 10
Dell(conf-if-te-2/3)#switchport mode private-vlan promiscuous
```

Related Commands

- private-vlan mode — sets the mode of the selected VLAN to community, isolated, or primary.
- private-vlan mapping secondary-vlan — sets the mode of the selected VLAN to primary and then associates the secondary VLANs to it.
- show interfaces private-vlan — displays type and status of PVLAN interfaces.

49

Quality of Service (QoS)

The Dell Networking operating software commands for quality of service (QoS) include traffic conditioning and congestion control.
This chapter contains the following sections:

- Global Configuration Commands
- Per-Port QoS Commands
- Policy-Based QoS Commands

Topics:

- Global Configuration Commands
- Per-Port QoS Commands
- Policy-Based QoS Commands
- DSCP Color Map Commands

Global Configuration Commands

The following QoS commands are enabled globally when configured on your switch.

qos-rate-adjust

Enable QoS rate adjustment to include overhead fields in rate metering calculations.

C9000 Series

Syntax `qos-rate-adjust overhead-bytes-number`

Parameters

overhead-bytes-number	Enter the number of bytes of packet overhead to include in rate limiting, policing, and shaping calculations. The range is from 1 to 31.

Defaults QoS rate adjustment is disabled by default.

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced.

Usage Information

By default, when rate policing and shaping, the system does not include the Preamble, SFD, or the IFG fields. These fields are overhead; only the fields from MAC destination address to the CRC are used for forwarding and are included in these rate metering calculations.

Use this command in Configuration Terminal Batch mode to enable the QoS rate adjustment in a dual-homing setup.

service-class bandwidth-percentage

Specify a minimum bandwidth for queues.

C9000 Series

Syntax

```
service-class bandwidth-percentage queue0 percentage queue1 percentage queue2
percentage queue3 percentagequeue4 percentage queue5 percentage queue6
percentage
```

Parameters

percentage	Enter the bandwidth-weight as a percentage. The range is from 1 to 100.

Defaults

none

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.1	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

Usage Information

Guarantee a minimum bandwidth to different queues globally using the `service-class bandwidth-percentage` command from CONFIGURATION mode. The command is applied in the same way as the `bandwidth-percentage` command in an output QoS policy. The `bandwidth-percentage` command in QOS-POLICY-OUT mode supersedes the `service-class bandwidth-percentage` command.

Use this command in Configuration Terminal Batch mode to specify the minimum bandwidth for queues in a dual-homing setup.

service-class dot1p-mapping

Configure a service-class criterion based on a dot1p value.

C9000 Series

Syntax

```
service-class dot1p-mapping {dot1p0 value | dot1p1 value | dot1p2 value |
dot1p3 value | dot1p4 value| dot1p5 value | dot1p6 value | dot1p7 value}
```

Parameters

dot1p0 *value* ... dot1p7 *value*	Enter a dot1p list number and value. The list number range is from 0 to 7. The range is from 0 to 7.

Defaults

For each dot1p Priority, the default CoS queue value is:

- Dot1p Priority: 0 1 2 3 4 5 6 7
- Queue: 1 0 2 3 4 5 6 7

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

To apply dot1p-queue-mapping, use the `service-class dynamic dot1p` command.

Use this command in Configuration Terminal Batch mode to apply the dot1p-queue-mapping in a dual-homing setup.

Related Commands

show qos dot1p-queue-mapping — displays the dot1p priority to queue mapping on the switch.

service-class dynamic dot1p

Honor all 802.1p markings on incoming switched traffic on an interface (from INTERFACE mode) or on all interfaces (from CONFIGURATION mode). A CONFIGURATION mode entry supersedes an INTERFACE mode entry.

C9000 Series

Syntax

`service-class dynamic dot1p`

To return to the default setting, use the `no service-class dynamic dot1p` command.

Defaults

All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command. The default mapping is as follows:

Table 8. Default Mapping

dot1p	Queue ID
0	1
1	0
2	2
3	3
4	4
5	5
6	6
7	7

Command Modes

INTERFACE

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added the `kbps` option on the C-Series, E-Series, and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Expanded the command to permit configuration on port channels.
6.1.1.1	Introduced on the E-Series.

Usage Information

To honor all incoming 802.1p markings on incoming switched traffic on the interface, enter this command. By default, this facility is not enabled (that is, the 802.1p markings on incoming traffic are not honored).

You can apply this command on both physical interfaces and port channels. When you set the service-class dynamic for a port channel, the physical interfaces assigned to the port channel are automatically configured; you cannot assign the `service-class dynamic` command to individual interfaces in a port channel.

- All dot1p traffic is mapped to Queue 0 unless you enable the `service-class dynamic dot1p` command on an interface or globally.
- Layer 2 or Layer 3 service policies supersede dot1p service classes.

Use this command in Configuration Terminal Batch mode to honor the incoming 802.1p markings in a dual-homing setup.

service-class wred backplane

After you create a WRED profile with ECN functionality, specify per-queue granularity for backplane ports and include the WRED profile in a service class. Using this command, you can enable or disable queue-specific settings and specify minimum and maximum buffer thresholds in the WRED profile applied to each packet color-code. Also, you can specify the maximum drop rate percentage for yellow and green profiles. The per-queue profile configured is applied to all the backplane ports.

C9000 Series

Syntax

```
[no] service-class wred {green | weight | yellow} {[queue0 number/string] ||
[queue1 number/string] || [queue2 number/string] || [queue3 number/string] ||
[queue4 number/string] || [queue5 number/string] || [queue6 number/string] ||
[queue7 number/string]} backplane
```

Parameters

service-class	Define the mapping between the service class and policy-based QoS or routing.
wred	Specify WRED curve parameters for a queue
green	Specify green (low) drop precedence to a queue.

weight	Specify a weight factor to a queue.
yellow	Specify yellow (medium) drop precedence to a queue.
queue 0 to queue 7	Specify the queue number to which the WRED parameters apply.
number	Enter a weight for the queue as a number in the range of 1 to 15. This parameter applies only if you specify the green or yellow drop precedence.
string	Enter the WRED profile name. It is a string of up to 32 characters. Or use one of the five pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_. This parameter applies only if you specify a weight factor.
backplane	Specify that the WRED weight and profile configured for each queue apply to backplane ports.

Default All queues on backplane ports operate in tail-drop (best-effort traffic) mode by default. There is no default WRED green or yellow profile. The default weight is 0.

Command Modes QOS-POLICY-OUT mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.1.0	Introduced on the Z9500 switch.
9.3.0.0	Introduced on the Z9000 platform.

Usage Information You can configure queues 0-7. WRED profile contains a set of characteristics, such as the minimum and maximum WRED thresholds and the maximum drop rate. You can add and remove WRED parameters for one or more queues by using the command in a single line. All of the configured attributes apply to all the backplane ports and are for each queue. To assign drop precedence to green or yellow traffic, use this command. If there is no honoring enabled on the input, all the traffic defaults to green drop precedence.

Example

```
Dell(conf-wred)#wred thresh-1
Dell(conf-wred)#threshold min 100 max 200 max-drop-rate 40
Dell(conf-wred)#wred thresh-2
Dell(conf-wred)#threshold min 300 max 400 max-drop-rate 80
Dell(conf)#service-class wred green queue5 thresh-1 queue7 thresh-2 backplane
Dell(conf)#service-class wred yellow queue1 thresh-2 queue3 thresh-1 backplane
Dell(conf)#service-class wred weight queue0 11 queue6 4 queue7 9 backplane
```

service-pool wred

Configure a global buffer pool that serves as a shared buffer accessed by multiple queues when the minimum guaranteed buffers for a queue are consumed.

The switch supports four global service-pools in the egress direction. Two service pools are used—one for lossy queues and the other for lossless (priority-based flow control (PFC)) queues. You can enable WRED and ECN operation on the global service-pools. You can define WRED profiles and weight on each of the global service-pools for both lossy and lossless (PFC) service-pools.

C9000 Series

Syntax `[no] buffer-pool wred {green | weight | yellow} {[pool0 number/string] || [pool1 number/string]}`

Parameters

buffer-pool	Define the mapping between the service class and policy-based QoS or routing.
wred	Specify WRED curve parameters for a queue.
green	Specify green (low) drop precedence to a queue.
weight	Specify a weight factor to a queue
yellow	Specify yellow (medium) drop precedence to a queue
pool0	Service-pool buffer 1 (default service-pool for PFC traffic)
pool1	Service-pool buffer 0 (default service-pool for lossy traffic)
number	Enter a weight for the queue as a number in the range of 1 to 15. This parameter applies only if you specify the green or yellow drop precedence.
string	Enter the WRED profile name. It is a string of up to 32 characters. Or use one of the five pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_. This parameter applies only if you specify a weight factor.

Default All queues on backplane ports operate in tail-drop (best-effort traffic) mode by default. There is no default WRED green or yellow profile. The default weight is 0.

Command Modes CONFIGURATION mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.1.0	Introduced on the Z9500 switch.
9.3.0.0	Introduced on the S6000 and Z9000 platforms.

Usage Information You can configure only service pools 0 and 1 because the Dell Networking OS uses only these two service pools. The service0 pool is used for lossy queues; the service1 pool is used for lossless (PFC) queues on all platforms.

You can configure the weight for the WRED average queue size on service1 pool on which PFC is supported; service0 pool does not support PFC.

A WRED profile contains a set of attributes, such as the minimum and maximum threshold values, and the maximum drop rate for the received packets. You can add or remove WRED parameter configurations for one or more shared service pools using a single command. The `buffer-pool wred` command is similar in usage and working to the `service-class bandwidth-percentage` *`queue-id`* command.

Example

```
Dell(conf-wred)#wred thresh-1
Dell(conf-wred)#threshold min 100 max 200 max-drop-rate 40

Dell(conf-wred)#wred thresh-2
Dell(conf-wred)#threshold min 300 max 400 max-drop-rate 80

Dell(conf)#service-pool wred green pool0 thresh-1 pool1 thresh-2
Dell(conf)#service-pool wred yellow pool0 thresh-3 pool1 thresh-4
Dell(conf #service-pool wred weight pool0 11 pool1 4
```

service-class wred ecn backplane

Apply ECN marking on backplane port-queues in a service class.

C9000 Series

Syntax `[no] service-class wred ecn queue-list backplane`

Parameters

service-class	Define the mapping between the service class and policy-based QoS or routing.
wred	Associate WRED with ECN to mark packets instead of dropping them.
ecn	Cause explicit congestion notification (ECN) to be used to indicate network congestion, rather than dropping packets, queues-list Enter the queue numbers, either as individual queue numbers separated by commas or as an inclusive list separating the starting and ending queue numbers with a hyphen
queue-list	Enter the port-queue numbers, either as individual queue numbers separated by commas or as an inclusive list separating the starting and ending queue numbers with a hyphen; for example, `service-class wred ecn 0, 2, 4-6 backplane`. The range of queue IDs is 0 to 7.
backplane	Specify that the ECN marking configured for each queue applies to backplane ports.

Default By default, ECN marking is disabled on all queues.

Command Modes CONFIGURATION mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.3.0.0	Introduced on the Z9500 switch.
9.3.0.0	Introduced on the Z9000 platform.

Usage Information You can add or remove ECN marking configuration on a list of queues on all backplane ports. All of the configured attributes apply to all the backplane ports and are for each queue. You can configure all the data queues. You can configure queues 0 to 7. By default, ECN marking is disabled on all queues. When you enable WRED with ECN and the number of packets in the queue is below the minimum threshold, packets are transmitted per the usual WRED treatment. When you enable WRED with ECN and the number of packets in the queue is between the minimum threshold and the maximum threshold, one of the following three scenarios can occur:

- If the transmission endpoints are ECN-capable and traffic is congested, and the WRED algorithm determines that the packet should be dropped based on the drop probability, the packet is transmitted and marked so the routers know the system is congested and can slow transmission rates.
- If neither endpoint is ECN-capable, the packet may be dropped based on the WRED drop probability. This behavior is the identical treatment that a packet receives when WRED is enabled without ECN configured on the router.
- If the network is experiencing congestion, the packet is transmitted. No further marking is required. When you enable WRED with ECN and the number of packets in the queue is above the maximum threshold, packets are dropped based on the drop probability. This behavior is the identical treatment a packet receives when WRED is enabled without ECN configured on the router.

Example

```
Dell(conf)#service-class wred ecn 0, 3-5, 7 backplane
```

show qos dot1p-queue-mapping

Displays the dot1p priority to queue mapping on the switch.

C9000 Series

Syntax

```
show qos dot1p-queue-mapping
```

Defaults

- dot1p Priority: 0 1 2 3 4 5 6 7
- Queue: 0 0 0 1 2 3 3 3

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.16.0	Introduced on MXL 10/40GbE Switch IO Module.

Related Commands

service-class dot1p-mapping — Identifies the class map.

Per-Port QoS Commands

Per-port QoS (port-based QoS) allows you to define the QoS configuration on a per-physical-port basis.

dot1p-priority

Assign a value to the IEEE 802.1p bits on the traffic this interface receives.

C9000 Series

Syntax

```
dot1p-priority priority-value
```

To delete the IEEE 802.1p configuration on the interface, use the `no dot1p-priority` command.

Parameters

priority-value	Enter a value from 0 to 7.

dot1p	Queue Number
0	1
1	0
2	2
3	3
4	4
5	5
6	6
7	7

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information The `dot1p-priority` command changes the priority of incoming traffic on the interface. The system places traffic marked with a priority in the correct queue and processes that traffic according to its queue.

When you set the priority for a port channel, the physical interfaces assigned to the port channel are configured with the same value. You cannot assign the `dot1p-priority` command to individual interfaces in a port channel.

rate police

Police the incoming traffic rate on the selected interface.

C9000 Series

Syntax `rate police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]] [vlan vlan-id]`

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps).
committed-rate	Enter the bandwidth in Mbps. The range is from 0 to 40000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is **50**.
peak *peak-rate*	(OPTIONAL) Enter the keyword `peak` then a number to specify the peak rate in Mbps. The range is from 0 to 40000.
vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then a VLAN ID to police traffic to those specific VLANs. The range is from 1 to 4094.

Defaults

Granularity for `commited-rate` and `peak-rate` is Mbps unless you use the `kbps` option.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added the `kbps` option on the C-Series, E-Series, and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

NOTE: Per Port rate limit and rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate limit and rate police is supported on only tagged ports with Layer 2 switched traffic.

On one interface, you can configure the `rate police` command for a VLAN or you can configure the `rate police` command for an interface. For each physical interface, you can configure three `rate police` commands specifying different VLANS.

Related Commands

rate-police — specifies traffic policing on the selected interface.

rate shape

Shape the traffic output on the selected interface.

C9000 Series

Syntax `rate shape [kbps] rate [burst-KB]`

Parameters

kbps	(Optional) Enter the keyword `kbps` to specify the rate limit in kilobits per second (Kbps). The range is from 0 to 10000000. The default granularity is Megabits per second (Mbps).
rate	Enter the outgoing rate in multiples of 10 Mbps. The range is from 0 to 40000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 0 to 10000. The default is 50.

Defaults Granularity for rate is **Mbps** unless you use the `kbps` option.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added the `kbps` option on the C-Series, E-Series, and S-Series.
7.6.1.0	Introduced on the S-Series and C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information If traffic is shaped between 64 and 1000 Kbs, for some values, the shaped rate is much less than the value configured.

Related Commands rate-shape — shapes traffic output as part of the designated policy.

Policy-Based QoS Commands

Policy-based traffic classification is handled with class maps. These maps classify unicast traffic into one of four classes. The system allows you to match multiple class maps and specify multiple match criteria. Policy-based QoS is not supported on logical interfaces, such as port-channels, VLANs, or loopbacks.

bandwidth-percentage

Assign a percentage of weight to the class/queue.

C9000 Series

Syntax

`bandwidth-percentage` *`percentage`*

To remove the bandwidth percentage, use the `no bandwidth-percentage` command.

Parameters

percentage	Enter the percentage assignment of weight to the class/queue. The range is from 1 to 100% (granularity 1%).

Defaults

none

Command Modes

CONFIGURATION (conf-qos-policy-out)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.1.9.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced on the E-Series.

Usage Information

The unit of bandwidth percentage is 1%. If the sum of the bandwidth percentages given to all eight classes exceeds 100%, the bandwidth percentage automatically scales down to 100%.

Related Commands

qos-policy-output — creates a QoS output policy.

buffer-stats-snapshot

Enable the buffer statistics tracking utility and enter the Buffer Statistics Snapshot configuration mode. You must enable this utility to be able to configure the parameters for buffer statistics tracking.

C9000

Syntax

`[No] buffer-stats-snapshot`

To disable the buffer statistics tracking utility, enter the `disable` command from the BUFFER-STATS-SNAPSHOT mode.

Default By default, buffer statistics tracking is disabled.

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3.0.0	Introduced on the S6000 platform

Usage Information Only the software-based trigger for retrieving and calculating the snapshots of the statistical counters of the buffer space is supported. Collection of snapshots of buffer statistical counters based on hardware threshold settings is not supported, which can be used to specify the type of hardware threshold and the threshold profile templates.

Use this command in Configuration Terminal Batch mode to enable the tracking utility in a dual-homing setup.

Example

```
Dell(conf)#buffer-stats-snapshot
Dell(conf-buffer-stats-snapshot)#?
disable                 Disable buffer-stats-snapshot globally
end                     Exit from configuration mode
exit                    Exit from buffer-stats-snapshot configuration mode
no                      Negate a command or set its defaults
show                    Show buffer-stats-snapshot configuration
Dell(conf-buffer-stats-snapshot)#no disable
Dell(conf-buffer-stats-snapshot)#show configuration
!
buffer-stats-snapshot
 no disable
```

class-map

Create a class map. Class maps differentiate traffic so that you can apply separate quality-of-service policies to each class.

C9000 Series

Syntax `class-map {match-all | match-any} class-map-name [layer2] [cpu-qos]`

Parameters

match-all	Determines how packets are evaluated when multiple match criteria exist. Enter the keywords `match-all` to determine that the packets must meet all the match criteria in order to be a member of the class.
match-any	Determines how packets are evaluated when multiple match criteria exist. Enter the keywords `match-any` to determine that the packets must meet at least one of the match criteria in order to be a member of the class.

class-map-name	Enter a name of the class for the class map in a character format (32 character maximum).
layer2	Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.
cpu-qos	Enter the keyword `cpu-qos` to create a class map to filter protocol traffic for rate-limiting control-plane traffic (CoPP).

Defaults Layer 3

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Class-map names can be 32 characters. Layer2 available on the C-Series and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Expanded to add support for Layer 2.

Usage Information Packets arriving at the input interface are checked against the match criteria and configured using this command to determine if the packet belongs to that class. This command accesses CLASS-MAP mode, where the configuration commands include the`match ip` and `match mac` options.

When you create a class map to filter protocol traffic for CoPP, you must enter the keyword `cpu-qos`.

Use this command in Configuration Terminal Batch mode to create the class map in a dual-homing setup.

Related Commands

- ip access-list extended — configures an extended IP ACL.
- match ip access-group — configures the match criteria based on the access control list (ACL).
- match ip precedence — identifies the IP precedence values as match criteria.
- match ip dscp — configures the match criteria based on the DSCP value.
- match mac access-group — configures a match criterion for a class map based on the contents of the designated MAC ACL.
- match mac dot1p — configures a match criterion for a class map based on a dot1p value.
- match mac vlan — configures a match criterion for a class map based on VLAN ID.
- service-queue — assigns a class map and QoS policy to different queues.

- show qos class-map — views the current class map information.

clear qos statistics

Clear Matched Packets through class maps applied to inbound ports

C9000 Series

Syntax `clear qos statistics interface-name`

Parameters

interface-name Enter one of the following keywords:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.18.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Related Commands show qos statistics — displays the QoS statistics.

description

Add a description to the selected policy map or QoS policy.

C9000 Series

Syntax

`description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the policies (80 characters maximum).

Defaults

none

Command Modes

CONFIGURATION (policy-map-input and policy-map-output; conf-qos-policy-in and conf-qos-policy-out; wred)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
pre-7.7.1.0	Introduced.

Related Commands

policy-map-input — creates an input policy map.

policy-map-output — creates an output policy map.

qos-policy-input — creates an input QoS-policy on the router.

qos-policy-output — creates an output QoS-policy on the router.

wred-profile — creates a WRED profile.

match ip access-group

Configure match criteria for a class map, based on the access control list (ACL).

C9000 Series

Syntax

`match ip access-group` *`access-group-name`* `[set-ip-dscp` *`value`*`]`

To remove ACL match criteria from a class map, use the `no match ip access-group access-group-name [set-ip-dscp value]` command.

Parameters

access-group-name	Enter the ACL name whose contents are used as the match criteria in determining if packets belong to the class the class-map specifies.
set-ip-dscp *value*	(OPTIONAL) Enter the keywords `set-ip-dscp` then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.

Defaults

none

Command Modes

CLASS-MAP CONFIGURATION (config-class-map)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added the `DSCP Marking` option support on the S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.5.1.0	Added support for the `DSCP Marking` option.
6.1.1.1	Introduced on the E-Series.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria. For class-map match-any, a maximum of five ACL match criteria are allowed. For `class-map match-all`, only one ACL match criteria is allowed.

Related Commands

class-map — identifies the class map.

match ip dscp

Use a differentiated services code point (DSCP) value as a match criteria.

C9000 Series

Syntax

`match {ip | ipv6 | ip-any} dscp dscp-list [set-ip-dscp value | set-color value]`

To remove a DSCP value as a match criteria, use the `no match {ip | ipv6 | ip-any} dscp dscp-list [[multicast] set-ip-dscp value | set-color value]` command.

Parameters

ip	Enter the keyword `ip` to support IPv4 traffic.
ipv6	Enter the keyword `ipv6` to support IPv6 traffic.
ip-any	Enter the keyword `ip-any` to support IPv4 and IPv6 traffic.
dscp-list	Enter the IP DSCP values that is to be the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). The range is from 0 to 63.
set-ip-dscp *value*	(OPTIONAL) Enter the keywords `set-ip-dscp` then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.
set-color *value*	(Optional) Enter the keyword set-color followed by a color value. Traffic that fulfills the match criteria is marked with the color value that you specify. The default value is yellow.

Defaults

none

Command Modes

CLASS-MAP CONFIGURATION (config-class-map)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added the `ipv6` and `ip-any` options on the Z9500.
9.5(0.0)	Added the `ipv6` and `ip-any` options on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added the keyword `multicast`. Added the `DSCP Marking` option support on the S-Series.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series. Added support for the `DSCP Marking` option.
6.2.1.1	Introduced on the E-Series.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

The `match ip dscp` and `match ip precedence` commands are mutually exclusive.

Up to 64 IP DSCP values can be matched in one match statement. For example, to indicate IP DCSP values 0 1 2 3 4 5 6 7, enter either the `match ip dscp 0,1,2,3,4,5,6,7` or `match ip dscp 0-7` command.

NOTE: Only one of the IP DSCP values must be a successful match criterion, not all of the specified IP DSCP values must match.

Related Commands

class-map — identifies the class map.

match ip precedence

Use IP precedence values as a match criteria.

C9000 Series

Syntax

`match {ip | ipv6 | ip-any} precedence ip-`*`precedence-list`* `[set-ip-dscp` *`value`* `| set-color` *`value`* `]`

To remove IP precedence as a match criteria, use the `no match {ip | ipv6 | ip-any} precedence ip-`*`precedence-list`* `[[multicast] set-ip-dscp` *`value`*`| set-color` *`value`* command.

Parameters

ip	Enter the keyword `ip` to support IPv4 traffic.
ipv6	Enter the keyword `ipv6` to support IPv6 traffic.
ip-any	Enter the keyword `ip-any` to support IPv4 and IPv6 traffic.
ip-precedence-list	Enter the IP precedence value(s) as the match criteria. Separate values by commas — no spaces (1,2,3) or indicate a list of values separated by a hyphen (1-3). The range is from 0 to 7.
set-ip-dscp *value*	(Optional) Enter the keywords `set-ip-dscp` then the IP DSCP value. The matched traffic is marked with the DSCP value. The range is from 0 to 63.
set-color *value*	(Optional) Enter the keyword set-color followed by a color value. Traffic that fulfills the match criteria is marked with the color value that you specify. The default value is Yellow.

Defaults

none

Command Modes

CLASS-MAP CONFIGURATION (config-class-map)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for the `ipv6` and `ip-any` options on the Z9500.
9.5(0.0)	Added support for the `ipv6` and `ip-any` options on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added the keyword `multicast`. Added support for the `DSCP marking` option for the S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.5.1.0	Added support for the `DSCP Marking` option.
6.1.1.1	Introduced on the E-Series.

Usage Information

To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

The `match ip precedence` command and the `match ip dscp` command are mutually exclusive.

Up to eight precedence values can be matched in one match statement. For example, to indicate the IP precedence values 0 1 2 3, enter either the `match ip precedence 0-3` or `match ip precedence 0,1,2,3` command.

NOTE: Only one of the IP precedence values must be a successful match criterion, not all of the specified IP precedence values must match.

Related Commands

class-map — identifies the class map.

match ip vlan

Uses a VLAN as the match criterion for an L3 class map.

C9000 Series

Syntax

`match ip vlan` *`vlan-id`*

To remove VLAN as the match criterion, use the `no match ip vlan` *`vlan-id`* command.

Parameters

vlan *vlan-id*	Enter the keyword vlan and then the ID of the VLAN. The range is from 1 to 4094.

Defaults none

Command Modes CONF-CLASS-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4.(0.0)	Introduced on the S-Series and Z-Series.

Usage Information To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.
Use this command to match an IP class-map against a single VLAN ID .

Related Commands class-map — identifies the class map.

match mac access-group

Configure a match criterion for a class map, based on the contents of the designated MAC ACL.

C9000 Series

Syntax `match mac access-group {mac-acl-name}`

Parameters

mac-acl-name	Enter a MAC ACL name. Its contents is used as the match criteria in the class map.

Defaults none

Command Modes CLASS-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
8.2.1.0	Available on the C-Series and S-Series.
7.5.1.0	Added support for the `DSCP Marking` option.
7.4.1.0	Introduced.

Usage Information To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

Related Commands class-map — identifies the class map.

match mac dot1p

Configure a match criterion for a class map based on a dot1p value.

C9000 Series

Syntax `match mac dot1p {dot1p-list}`

Parameters

dot1p-list	Enter a dot1p value. The range is from 0 to 7.

Defaults none

Command Modes CLASS-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Available on the C-Series and S-Series.
7.5.1.0	Added support for the `DSCP Marking` option.
7.4.1.0	Introduced.

Usage Information To access this command, enter the `class-map` command. After the class map is identified, you can configure the match criteria.

Related Commands class-map — identifies the class map.

match mac vlan

Configure a match criterion for a class map based on VLAN ID.

C9000 Series

Syntax `match mac vlan number`

Parameters

number	Enter the VLAN ID. The range is from 1 to 4094.

Defaults none

Command Modes CLASS-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced.

Usage Information To access this command, enter the `class-map` command. You can match against only one VLAN ID.

Related Commands class-map — identifies the class map.

policy-aggregate

Allow an aggregate method of configuring per-port QoS via policy maps. An aggregate QoS policy is part of the policy map (input/output) applied on an interface.

C9000 Series

Syntax `policy-aggregate qos-policy-name`

To remove a policy aggregate configuration, use the `no policy-aggregate qos-policy-name` command.

Parameters

qos-policy-name	Enter the name of the policy map in character format (32 characters maximum).

Defaults none

Command Modes CONFIGURATION (policy-map-input and policy-map-output)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Policy name character limit increased from 16 to 32.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information An aggregate output QoS policy applies to all outbound port traffic. An aggregate output QoS policy can coexist with per-queue output QoS policies.

Related Commands policy-map-input — creates an input policy map.

policy-map-output — creates an output policy map.

policy-map-input

Create an input policy map.

C9000 Series

Syntax `policy-map-input` *`policy-map-name`* `[layer2] [cpu-qos]`

To remove an input policy map, use the `no policy-map-input` *`policy-map-name`* `[layer2] [cpu-qos]` command.

Parameters

policy-map-name	Enter the name of the policy map in character format (32 characters maximum).
layer2	(OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.
cpu-qos	(OPTIONAL) Enter the keyword `cpu-qos` to create an input policy to be used to rate-limit control-plane traffic (CoPP).

Defaults **Layer 3**

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Policy name character limit increased from 16 to 32.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Expanded to add support for Layer 2.
6.1.1.1	Introduced on the E-Series.

Usage Information

The input policy map is used to classify incoming traffic to different flows using class-map, QoS policy, or incoming packets DSCP. This command enables Policy-Map-Input Configuration mode (conf-policy-map-in).

When you configure an input policy map for CoPP, you must enter the keyword `cpu-qos`.

Use this command in Configuration Terminal Batch mode to create an input policy map in a dual-homing setup.

Related Commands

service-queue — assigns a class map and QoS policy to different queues.

policy-aggregate — allows an aggregate method of configuring per-port QoS using policy maps.

service-policy input — applies an input policy map to the selected interface.

policy-map-output

Create an output policy map.

C9000 Series

Syntax

`policy-map-output` *`policy-map-name`*

To remove a policy map, use the `no policy-map-output` *`policy-map-name`* command.

Parameters

policy-map-name Enter the name for the policy map in character format (32 characters maximum).

Defaults

none

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Policy name character limit increased from 16 to 32.
7.6.1.0	Introduced on the C-Series and S-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

To assign traffic to different flows using QoS policy, use the Output Policy map. This command enables Policy-Map-Output Configuration mode (conf-policy-map-out).

Use this command in Configuration Terminal Batch mode to create the Output Policy map in a dual-homing setup.

Related Commands

service-queue — assigns a class map and QoS policy to different queues.

policy-aggregate — allows an aggregate method of configuring per-port QoS using policy maps.

service-policy output — applies an output policy map to the selected interface.

qos-policy-input

Create a QoS input policy on the router.

C9000 Series

Syntax

`qos-policy-input` *`qos-policy-name`* `[layer2] [cpu-qos]`

To remove an existing input QoS policy from the router, use the `no qos-policy-input` *`qos-policy-name`* `[layer2] [cpu-qos]` command.

Parameters

qos-policy-name	Enter the name for the policy map in character format (32 characters maximum).
layer2	(OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.
cpu-qos	Enter the keyword `cpu-qos` to create a QoS input policy to be used to rate-limit control-plane traffic (CoPP).

Defaults

Layer 3

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Policy name character limit increased from 16 to 32.
7.6.1.0	Introduced on the C-Series and S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

To specify the name of the input QoS policy, use this command. After the input policy is specified, rate-police is defined. This command enables Qos-Policy-Input Configuration mode — (conf-qos-policy-in).

When changing a Service-Queue configuration in a QoS policy map, all QoS rules are deleted and re-added automatically to ensure that the order of the rules is maintained. As a result, the Matched Packets value shown in the `show qos statistics` command is reset.

If you create create a QoS input policy to be used for CoPP, you must enter the keyword `cpu-qos`.

Use this command in Configuration Terminal Batch mode to create the QoS input policy in a dual-homing setup.

Related Commands

rate police — incoming traffic policing function.

qos-policy-output

Create a QoS output policy.

C9000 Series

Syntax

`qos-policy-output` *`qos-policy-name`*

To remove an existing output QoS policy, use the `no qos-policy-output` *`qos-policy-name`* command.

Parameters

qos-policy-name	Enter your output QoS policy name in character format (32 characters maximum).

Defaults

none

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Policy name character limit increased from 16 to 32.
7.6.1.0	Introduced on the C-Series and S-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

To specify the name of the output QoS policy, use this command. After the output policy is specified, rate-shape, bandwidth-percentage, and WRED can be defined. This command enables Qos-Policy-Output Configuration mode — (conf-qos-policy-out).

Use this command in Configuration Terminal Batch mode to create the QoS output policy in a dual-homing setup.

Related Commands

rate shape — rate-shape traffic functionality.

bandwidth-percentage — assigns weight to the class/queue percentage.

wred — assigns yellow or green drop precedence.

rate-police

Specify the policing functionality on incoming traffic.

C9000 Series

Syntax `rate-police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]]`

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in Kilobits per second (Kbps). Make the following value a multiple of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
committed-rate	Enter the bandwidth in Mbps. The range is from 0 to 40000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 16 to 200000. The default is **100**.
peak *peak-rate*	(OPTIONAL) Enter the keyword `peak` then a number to specify the peak rate in Mbps. The range is from 0 to 40000. The default is the same as designated for `committed-rate`.

Defaults Burst size is 100KB. `peak-rate` is by default the same as `committed-rate`. Granularity for `committed-rate` and `peak-rate` is Mbps unless you use the `kbps` option.

Command Modes QOS-POLICY-IN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added the `kbps` option on the C-Series, E-Series, and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information The default burst size is 100Kb. If a different value is required, you must configure the burst size to the required value.

Related Commands rate shape — shapes traffic output as part of the designated policy.

qos-policy-input — creates a QoS output policy.

rate-shape

Shape traffic output as part of an output QoS policy.

C9000 Series

Syntax

```
rate-shape {kbps | pps} peak-rate {burst-kbps | burst-packets} [committed {kbps | pps} committed-rate {burst-kbps | burst-packets}]
```

Parameters

kbps	Enter the keyword `kbps` to specify the rate limit in kilobits per second (Kbps) in multiples of 64. The default granularity is Megabits per second (Mbps).The range is from 0 to 40000000.
pps	Enter the keyword `pps` to specify the rate limit in packets per second (pps).The range is from 1-268000000.
committed	Enter the keyword to specify the committed rate.
burst-kbps	[Optional] Enter the peak rate or committed rate size in kilobits per second. The range is from 0-10000 . The default is 50.
burst-packets	[Optional] Enter the peak rate or committed rate size in packets per second. The range is from 1-1073000. The default is 200.

Command Modes

QOS-POLICY-OUT

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(1.0)	Added support for packets-per-second and committed rate.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added the `kbps` option on the C-Series, E-Series, and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information

You must configure the peak rate and peak burst size using the same value: kilobits or packets per second. Similarly, you must configure the committed rate and committed burst size with the same measurement.

Peak rate refers to the maximum rate for traffic arriving or exiting an interface under normal traffic conditions. Peak burst size indicates the maximum size of unused peak bandwidth that is aggregated. This aggregated bandwidth enables brief durations of burst traffic that exceeds the peak rate and committed burst.

Committed rate refers to the guaranteed bandwidth for traffic entering or leaving the interface under normal network conditions. When traffic propagates at an average rate that is less than or equal to the committed rate, it is considered to be green-colored or coded. When the transmitted traffic falls below the committed rate, the bandwidth, which is not used by any traffic that is traversing the network, is aggregated to form the committed burst size. Traffic is considered to be green-colored up to the point at which the unused bandwidth does not exceed the committed burst size.

Related Commands

qos-policy-output — creates a QoS output policy.

rate police — specifies traffic policing on the selected interface.

service-class buffer shared-threshold-weight

Create a service class and associate the threshold weight of the shared buffer with each of the queues per port in the egress direction. A global buffer pool that is a shared buffer pool accessed by multiple queues when the minimum guaranteed buffers for the queue are consumed can be configured on the switch.

C9000 Series

Syntax

```
[No] Service-class buffer shared-threshold-weight {[queue0 number] || [queue1 number] || [queue2 number] || [queue3 number] || [queue4 number] || [queue5 number] || [queue6 number] || [queue7 number]}
```

Parameters

buffer	Define the shared buffer settings
shared-threshold-weight	Specify the weight of a queue for the shared buffer space
queue 0 to queue 7	Specify the queue number to which the WRED parameters apply
number	Enter a weight for the queue on the shared buffer as a number in the range of 1 to 11.

Default

The default threshold weight on the shared buffer for each queue is 9. Therefore, each queue can consume up to 66.67 percent of available shared buffer by default.

Command Modes

INTERFACE mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S6000 platform

Usage Information

You can configure all the data queues. For S6000, you can configure queues 0-7.

The following table describes the mapping between the threshold weight of the shared buffer on the queue and the percentage of available shared buffer that is used by the queue for each of the corresponding threshold weights of the shared buffer:

shared-threshold-weight on the queue	% of available shared buffer that can be consumed by the queue.
0	No dynamic sharing; shared buffer = 0.
1	0.77%
2	1.54%
3	3.03%
4	5.88%
5	11.11%
6	20%
7	33.33%
8	50%
9	66.67%
10	80%
11	88.89%

Example

```
Dell(conf-if-te-0/8)#service-class buffer shared-threshold-weight queue5 4
queue7 6
```

service-policy input

Apply an input policy map to the selected interface.

C9000 Series

Syntax `service-policy input` *`policy-map-name`* `[layer2]`

To remove the input policy map from the interface, use the `no service-policy input policy-map-name [layer2]` command.

Parameters

policy-map-name	Enter the name for the policy map in character format (32 characters maximum). You can identify an existing policy map or name one that does not yet exist.
layer2	(OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults **Layer 3**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Expanded to add support for Layer 2.
6.1.1.1	Introduced on the E-Series.

Usage Information You can attach a single policy-map to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

NOTE: The `service-policy` commands are not allowed on a port channel. The `service-policy input policy-map-name` command and the `service-class dynamic dot1p` command are not allowed simultaneously on an interface. However, the `service-policy input` command (without the `policy-map-name` option) and the `service-class dynamic dot1p` command are allowed on an interface.

Related Commands policy-map-input — creates an input policy map.

service-policy output

Apply an output policy map to the selected interface.

C9000 Series

Syntax `service-policy output` *`policy-map-name`*

To remove the output policy map from the interface, use the `no service-policy output` *`policy-map-name`* command.

Parameters

policy-map-name	Enter the name for the policy map in character format (32 characters maximum). You can identify an existing policy map or name one that does not yet exist.

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces. A policy map attached to an interface can be modified.

Related Commands policy-map-output — creates an output policy map.

service-queue

Assign a class map and QoS policy to different queues.

C9000 Series

Syntax `service-queue` *`queue-id`* `[class-map` *`class-map-name`*`] [qos-policy` *`qos-policy-name`*`]`

To remove the queue assignment, use the `no service-queue` *`queue-id`* `[class-map` *`class-map-name`*`] [qos-policy` *`qos-policy-name`*`]` command.

Parameters

queue-id	Enter the value used to identify a queue. The range is from 0 to 7.
class-map *class-map-name*	(OPTIONAL) Enter the keyword `class-map` then the class map name assigned to the queue in character format (32 character maximum). **NOTE: This option is available under `policy-map-input` only.**
qos-policy *qos-policy-name*	(OPTIONAL) Enter the keywords `qos-policy` then the QoS policy name assigned to the queue in text format (32 characters maximum). This specifies the input QoS policy

assigned to the queue under `policy-map-input` and output QoS policy under `policy-map-output` context.

Defaults none

Command Modes CONFIGURATION (conf-policy-map-in and conf-policy-map-out)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information This command assigns a class map or QoS policy to different queues. There are eight queues per interface on the Z9500.

Related Commands

- class-map— identifies the class map.
- service-policy input— applies an input policy map to the selected interface.
- service-policy output— applies an output policy map to the selected interface.

set

Mark outgoing traffic with a differentiated service code point (DSCP) or dot1p value.

C9000 Series

Syntax `set {ip-dscp value | mac-dot1p value}`

Parameters

ip-dscp *value*	(OPTIONAL) Enter the keywords `ip-dscp` then the IP DSCP value. The range is from 0 to 63.
mac-dot1p *value*	Enter the keywords `mac-dot1p` then the dot1p value. The range is from 0 to 7.

Defaults none

Command Modes CONFIGURATION (conf-qos-policy-in)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Added `mac-dot1p` on the C-Series and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added support for `mac-dot1p`.
6.1.1.1	Introduced on the E-Series.

Usage Information

After the IP DSCP bit is set, other QoS services can then operate on the bit settings.

show qos class-map

View the current class map information.

C9000 Series

Syntax

```
show qos class-map [class-name]
```

Parameters

class-name	(Optional) Enter the name of a configured class map.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos class-map

Class-map match-any CM
  Match ip access-group ACL
```

Related Commands class-map — identifies the class map.

show qos policy-map

View the QoS policy map information.

C9000 Series

Syntax `show qos policy-map {summary [interface] | detail [interface]}`

Parameters

summary *interface* To view a policy map interface summary, enter the keyword `summary` and optionally one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

detail *interface* To view a policy map interface in detail, enter the keyword `detail` and optionally one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255;

the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series only: Added `Trust IPv6 diffserv`.
6.2.1.1	Introduced on the E-Series.

Example (IPv4)

```
Dell#show qos policy-map detail tengigabitethernet 1/1

Interface TenGigabitEthernet 1/1

Policy-map-input policy
Trust diffserv
Queue# Class-map-name Qos-policy-name
 0 - q0
 1 CM1q1
 2 CM2q2
 3 CM3q3
 4 CM4q4
 5 CM5q5
 6 CM6q6
 7 CM7q7
Dell#
```

Example (IPv6)

```
Dell# show qos policy-map detail tengigabitethernet 0/10

Interface TengigabitEthernet 0/10

Policy-map-input pmap1
Queue# Class-map-name Qos-policy-name
 0       c0            q0
 1       c1            q1
 2       c2            q2
 3       c3            q3
 4       c4            q4
```

```
 5       c5             -
 6       c6             q6
 7       c7             q7
Dell#
```

Example (Summary IPv4)

```
Dell#sho qos policy-map summary

Interface policy-map-input policy-map-output
Te 2/1     PM1                 -
Te 2/2     PM2         PMOut
Dell#
```

show qos policy-map-input

View the input QoS policy map details.

C9000 Series

Syntax `show qos policy-map-input [policy-map-name] [class class-map-name] [qos-policy-input qos-policy-name]`

Parameters

policy-map-name	Enter the policy map name.
class *class-map-name*	Enter the keyword `class` then the class map name.
qos-policy-input *qos-policy-name*	Enter the keyword `qos-policy-input` then the QoS policy name.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added Trust IPv6 diffserv.

pre-6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos policy-map-input

Policy-map-input PolicyMapInput
Aggregate Qos-policy-name AggPolicyIn
Queue# Class-map-name  Qos-policy-name
0      ClassMap1       qosPolicyInput
Dell#
```

Example

```
Dell# show qos policy-map-input

Policy-map-input pmap1
Trust ipv6-diffserv
Queue#  Class-map-name  Qos-policy-name
0       c0              q0
1       c1              q1
2       c2              q2
3       c3              q3
4       c4              q4
5       c5              -
6       c6              q6
7       c7              q7
Dell#
```

show qos policy-map-output

View the output QoS policy map details.

C9000 Series

Syntax `show qos policy-map-output [policy-map-name] [qos-policy-output qos-policy-name]`

Parameters

policy-map-name	Enter the policy map name.
qos-policy-output *qos-policy-name*	Enter the keyword `qos-policy-output` then the QoS policy name.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos policy-map-output

Policy-map-output PolicyMapOutput
Aggregate Qos-policy-name AggPolicyOut
Queue#   Qos-policy-name
  0      qosPolicyOutput
Dell#
```

show qos qos-policy-input

View the input QoS policy details.

C9000 Series

Syntax `show qos qos-policy-input [qos-policy-name]`

Parameters

qos-policy-name	Enter the QoS policy name.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos qos-policy-input

Qos-policy-input QosInput
        Rate-police 100 50 peak 100 50
        Dscp 32
Dell#
```

show qos qos-policy-output

View the output QoS policy details.

C9000 Series

Syntax `show qos qos-policy-output [qos-policy-name]`

Parameters

qos-policy-name	Enter the QoS policy name.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos qos-policy-output

Qos-policy-output qosOut
        Rate-limit 50 50 peak 50 50
        Wred yellow 1
        Wred green 1
```

show qos statistics

View QoS statistics.

C9000 Series

Syntax `show qos statistics {wred-profile [interface]} | [interface]`

Parameters

wred-profile *interface*

Enter the keywords `wred-profile` and optionally one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40–Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

interface

Enter one of the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40–Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id* / stack-unit / port-id information.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.1	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.1	Introduced on the E-Series.

Usage Information In a dual homing setup, you can use this command only from the primary VLT peer.

Example

```
DELL#show qos statistics peGigE 0/1/1
Interface peGigE 0/1/1
Queue# Matched Pkts
  0      0
  1      0
  2      0
  3      0
  4      0
  5      0
  6      0
  7      0

DELL#show qos statistics wred-profile peGigE 0/1/1
Interface peGigE 0/1/1
Drop-statistic Dropped Pkts
Green           0
Yellow          0
Out of Profile 0
```

show qos wred-profile

View the WRED profile details.

C9000 Series

Syntax `show qos wred-profile wred-profile-name`

Parameters

wred-profile-name	Enter the WRED profile name to view the profile details.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.1.1.1	Introduced on the E-Series.

Example

```
Dell#show qos wred-profile

Wred-profile-name        min-threshold  max-threshold  max-drop-rate
wred_drop                    0              0            100
wred_teng_y                594           5941            100
wred_teng_g                594           5941             50
wred_fortyg_y              594           5941             50
wred_fortyg_g              594           5941             25
wred_oneg_y_pe             154           1538            100
wred_oneg_g_pe             154           1538             50
wred_teng_y_pe             154           1538             50
wred_teng_g_pe             154           1538             25
Dell#
```

threshold

Specify the minimum and maximum threshold values for the configured WRED profiles.

C9000 Series

Syntax

`threshold min` *number* `max` *number*

To remove the threshold values, use the `no threshold min` *number* `max` *number* command.

Parameters

min *number*	Enter the keyword `min` then the minimum threshold number for the WRED profile. The range is from 0 to 12000KB.
max *number*	Enter the keyword `max` then the maximum threshold number for the WRED profile. The range is from 0 to 12000KB.

Defaults

none

Command Modes

CONFIGURATION (config-wred)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.
6.1.1.1	Introduced on the E-Series.

Usage Information To configure the minimum and maximum threshold values for user-defined profiles, use this command. Additionally, to modify the minimum and maximum threshold values for the pre-defined WRED profiles, use this command. If you delete the threshold values of the pre-defined WRED profiles, the profiles revert to their original default values.

Table 9. Threshold Values for the Pre-defined WRED Profiles

Pre-Defined WRED Profile Name	Minimum Threshold	Maximum Threshold
wred_drop	0	0
wred_ge_y	1024	2048
wred_ge_g	2048	4096
wred_teng_y	4096	8192
wred_teng_g	8192	16384

Related Commands wred-profile — creates a WRED profile.

trust

Specify dynamic classification (DSCP) or dot1p to trust.

C9000 Series

Syntax `trust {diffserv [fallback]| dot1p [fallback]}`

Parameters

diffserv	Enter the keyword `diffserv` to specify trust of DSCP markings.
dot1p	Enter the keyword `dot1p` to specify trust dot1p configuration.
fallback	Enter the keyword `fallback` to classify packets according to their DSCP value as a secondary option in case no match occurs against the configured class maps.

Defaults none

Command Modes CONFIGURATION (conf-policy-map-in)

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added `fallback` to the E-Series.
8.2.1.0	Added `dot1p` to the C-Series and S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added `dot1p` and `IPv6 DSCP`.
6.1.1.1	Introduced on the E-Series

Usage Information

When you configure `trust`, matched bytes/packets counters are not incremented in the `show qos statistics` command.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The following lists the default mapping.

Table 10. Default Mapping

DSCP/CP hex Range (XXX)	DSCP Definition	Traditional IP Precedence	C9010 Internal Queue ID	DSCP/CP Decimal
111XXX		Network Control	7	48–63
110XXX		Internetwork Control	6	48–63
101XXX	EF (Expedited Forwarding)	CRITIC/ECP	5	32–47
100XXX	AF4 (Assured Forwarding)	Flash Override	4	32–47
011XXX	AF3	Flash	3	16–31
010XXX	AF2	Immediate	2	16–31
001XXX	AF1	Priority	1	0–15
000XXX	BE (Best Effort)	Best Effort	0	0–15

wred

Configure a WRED profile for yellow or green traffic.

C9000 Series

Syntax `wred {yellow | green} profile-name`

To remove the WRED drop precedence, use the no wred {yellow | green} [*profile-name]* command.

Parameters

yellow | green	Enter the keyword `yellow` for yellow traffic. A DSCP value of xxx100, xxx101, and xxx110 maps to yellow. Enter the keyword green for `green` traffic. A DSCP value of xxx0xx maps to green.
profile-name	Enter your WRED profile name in character format (32 character maximum). Or use one of the five pre-defined WRED profile names. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_.

Defaults none

Command Modes QOS-POLICY-OUT mode

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Profile name character limit increased from 16 to 32.
6.1.1.1	Introduced on the .E-Series

Usage Information To assign drop precedence to green or yellow traffic, use this command. If there is no honoring enabled on the input, all the traffic defaults to green drop precedence.

Related Commands wred-profile — creates a WRED profile and name that profile.

trust — defines the dynamic classification to trust DSCP.

wred weight

Configure the weight factor used to determine the average-queue size for WRED and ECN operation. The weight value is used in an output QoS policy applied to a front-end or backplane port.

C9000 Series

Syntax `[no] wred weight` *`number`*

Parameters

weight	Define the weight factor to be used for computation of the WRED average-queue size to either enable WRED to discard packets or cause ECN to mark packets that exceed the minimum threshold configured. This setting applies to front-end and backplane ports.
number	Enter the weight as a number to be used to calculate the average-queue size. The range is 1 to 15. The default is 0.

Default The default weight is zero.

Command Modes QOS-POLICY-OUT mode

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.1.0	Introduced on the Z9500 switch.
9.3.0.0	Introduced on the S6000 and Z9000 platforms

Usage Information If the average queue size is more than the maximum threshold of WRED, the packet is dropped. If the average queue size is between the minimum and maximum threshold values, the decision to drop or queue the packet is taken based on the packet drop probability. The probability that a packet is dropped depends on the minimum threshold, maximum threshold, and mark probability denominator.

Example

```
Dell(conf-qos-policy-out)# wred weight 5
```

wred ecn

To indicate network congestion without dropping packets, use explicit congestion notification (ECN).

C9000 Series

Syntax `wred ecn`

To stop marking packets, use the `no wred ecn` command.

Defaults none

Command Modes QOS-POLICY-OUT mode

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820t.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.

Usage Information

When you enable `wred ecn`, and the number of packets in the queue is below the minimum threshold, packets are transmitted per the usual WRED treatment.

When you enable `wred ecn`, and the number of packets in the queue is between the minimum threshold and the maximum threshold, one of the following scenarios can occur:

- If the transmission endpoints are ECN-capable and traffic is congested, and the WRED algorithm determines that the packet should have been dropped based on the drop probability, the packet is transmitted and marked so the routers know the system is congested and can slow transmission rates.
- If neither endpoint is ECN-capable, the packet may be dropped based on the WRED drop probability. This behavior is the identical treatment that a packet receives when WRED is enabled without ECN configured on the router.

When you enable `wred ecn`, and the number of packets in the queue is above the maximum threshold, packets are dropped based on the drop probability. This behavior is the identical treatment a packet receives when WRED is enabled without ECN configured on the router.

Related Commands

wred-profile — creates a WRED profile and name that profile.

wred-profile

Create a WRED profile and name the profile.

C9000 Series

Syntax

`wred-profile` *`wred-profile-name`*

To remove an existing WRED profile, use the `no wred-profile` command.

Parameters

wred-profile-name	Enter your WRED profile name in character format (32 character maximum). Or use one of the pre-defined WRED profile names. You can configure up to 26 WRED profiles plus the five pre-defined profiles, for a total of 31 WRED profiles. Pre-defined Profiles: wred_drop, wred-ge_y, wred_ge_g, wred_teng_y, wred_teng_g.

Defaults

The five pre-defined WRED profiles. When you configure a new profile, the minimum and maximum threshold defaults to predefined wred_ge_g values.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.1.1.1	Introduced on the E-Series

Usage Information

Use the default pre-defined profiles or configure your own profile. You cannot delete the pre-defined profiles or their default values. This command enables WRED configuration mode —(conf-wred).

Use this command in Configuration Terminal Batch mode to create the WRED profile in a dual-homing setup.

Related Commands

threshold — specifies the minimum and maximum threshold values of the WRED profile.

show hardware

This command displays hardware buffer configurations and counters.

C9000 Series

Syntax

```
show hardware {linecard number | pe-unit number stack-unit number} buffer unit number port number buffer-info
```

Parameters

linecard	Line card 0 – 11.
pe-unit	PE-unit is use to specify the PE. PE ID 1 – 255.
stack-unit	Stack-unit is used to specify the statck unite in the stacked PE system. Stack-unit within a PE ID 0 – 7.
buffer-unit	Buffer unit is used to specify the port-pipe. Buffer-unit 0 – 0.

Defaults

None

Command Modes

Exec

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

DSCP Color Map Commands

The DSCP color map allows you to set the number of specific DSCP values to yellow or red. Traffic marked as yellow delivers traffic to the egress queue which will either transmit the packet if it has available bandwidth or drop the packet due to no ability to send. Traffic marked as red (high drop precedence) is dropped.

dscp

Sets the number of specific DSCP values for a color map profile to yellow or red.

C9000 Series

Syntax

`dscp {yellow | red} [list-dscp-values]`

To remove a color policy map profile, use the `no dscp {yellow | red} [dscp-list]` command.

Parameters

Yellow	Enter the `yellow` keyword. Traffic marked as yellow delivers traffic to the egress queue which either transmits the packet if it has available bandwidth or drops the packet due to no ability to send.
red	Enter the `red` keyword. Traffic marked as red is dropped.
dscp-list	Enter a list of IP DSCP values. The *dscp-list* parameter specifies the full list of IP DSCP value(s) for the specified color. Each DSCP value in a list is separate values by commas – no spaces (1,2,3) or indicates a list of values separated by a hyphen (1-3). Range is `0` to `63`.

Defaults **None**

Command Modes CONFIG-COLOR-MAP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information If the specified color-map does not exist, the Diffserv Manager (DSM) creates a color map and sets all the DSCP values to green (low drop precedence).

The default setting for each DSCP value (0-63) is green (low drop precedence). This command allows setting the number of specific DSCP values to yellow or red.

Important Points to Remember

- All DSCP values that are not specified as yellow or red are colored green.
- A DSCP value cannot be in both the yellow and red lists. Setting the red or yellow list with any DSCP value that is already in the other list results in an error and no update to that list is made.
- Each color map can only have one list of DSCP values for each color; any DSCP values previously listed for that color that are not in the new DSCP list are colored green.

Example

```
Dell(conf-dscp-color-map)# dscp yellow 9,10,11,13,15,16
```

Related Commands

qos dscp-color-map — configures the DSCP color map

qos dscp-color-policy— configures a DSCP color policy

qos dscp-color-map

Configure the DSCP color map.

C9000 Series

Syntax

`qos dscp-color-map` *`map-name`*

To remove a color map, use the no `qos dscp-color-map` *map-name* command.

Parameters

map-name	Enter the name of the DSCP color map. The map name can have a maximum of 32 characters.

Defaults

None

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information

A color map outlines the codepoint mappings to the appropriate color mapping (green, yellow, red) for the traffic. The system uses this information use to handle the traffic on the interface based on the traffic priority and places it into the appropriate shaping queue. You cannot delete a DSCP color map when it is configured on an interface. If you do, all the DSCP values are set to green (low drop precedence). To delete the DSCP color map that is being used by one or more interfaces, remove the DSCP map from each interface.

Use this command in Configuration Terminal Batch mode to configure the DSCP color map in a dual-homing setup.

Example

```
Dell(conf)#qos dscp-color-map mymap
```

Related Commands

qos dscp-color-map— associates the DSCP color map profile with an interface so that all IP packets received on it is given a color based on that color map

dscp— sets the number of specific DSCP values for color map profile to yellow or red.

qos dscp-color-policy

Associates the DSCP color map profile with an interface so that all IP packets received on it is given a color based on that color map.

C9000 Series

Syntax

`dscp-color-policy` *color-map-profile-name*

To remove a color policy map profile, use the no `dscp-color-policy` *color-map-profile-name* command.

Parameters

color-map-profile-name	Enter the color map profile name. The name can have a maximum of 32 characters.

Defaults

None

Command Modes

CONFIG-INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information

If the specified color-map does not exist, the Diffserv Manager (DSM) creates a color map and sets all the DSCP values to green (low drop precedence).

Example

The following example assigns the color map, **bat-enclave-map**, to interface **te 0/11**.

```
Dell(conf)# int te 0/11
Dell(conf-if-te-0/11)# qos dscp-color-policy bat-enclave-map
```

Related Commands dscp— sets the number of specific DSCP values for color map profile to yellow or red.

qos dscp-color-map— configures the DSCP color map.

show qos dscp-color-map

Display the DSCP color map for one or all interfaces.

C9000 Series

Syntax `show qos dscp-color-map map-name`

Parameters

map-name	Enter the name of the color map.

Defaults **None**

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Example

```
Display all DSCP color maps.

Dell# show qos dscp-color-map
Dscp-color-map mapONE
  yellow 4,7
  red 20,30
Dscp-color-map mapTWO
  yellow 16,55

Display a specific DSCP color map.

Dell# show qos dscp-color-map mapTWO
Dscp-color-map mapTWO
  yellow 16,55
```

Related Commands qos dscp-color-map— Configures a DSCP color map.

50

Rapid Spanning Tree Protocol (RSTP)

The Dell Networking operating software implementation of rapid spanning tree protocol (RSTP) is based on the IEEE 802.1w standard spanning-tree protocol. The RSTP algorithm configures connectivity throughout a bridged local area network (LAN) that is comprised of LANs interconnected by bridges.

Topics:

- bridge-priority
- debug spanning-tree rstp
- description
- disable
- forward-delay
- hello-time
- max-age
- protocol spanning-tree rstp
- show config
- show spanning-tree rstp
- spanning-tree rstp
- tc-flush-standard

bridge-priority

Set the bridge priority for RSTP.

C9000 Series

Syntax

`bridge-priority` *priority-value*

To return to the default value, use the `no bridge-priority` command.

Parameters

priority-value	Enter a number as the bridge priority value in increments of 4096. The range is from 0 to 61440. The default is **32768**.

Defaults

32768

Command Modes

CONFIGURATION RSTP (conf-rstp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands protocol spanning-tree rstp — enters rapid spanning tree mode.

debug spanning-tree rstp

Enable debugging of RSTP and view information on the protocol.

C9000 Series

Syntax `debug spanning-tree rstp [all | bpdu interface {in | out} | events]`

To disable debugging, use the `no debug spanning-tree rstp` command.

Parameters

all	(OPTIONAL) Enter the keyword `all` to debug all spanning tree operations.
bpdu *interface* {in | out}	(OPTIONAL) Enter the keyword `bpdu` to debug the bridge protocol data units. (OPTIONAL) Enter the keyword `interface` along with the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. Optionally, enter an in or out parameter with the optional interface: • For Receive, enter `in`. • For Transmit, enter `out`.
events	(OPTIONAL) Enter the keyword `events` to debug RSTP events.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell#debug spanning-tree rstp bpdu tengigabitethernet 2/0 ?
in Receive (in)
out Transmit (out)
```

description

Enter a description of the rapid spanning tree.

C9000 Series

Syntax `description {description}`

To remove the description, use the `no description {description}` command.

Parameters

description	Enter a description to identify the rapid spanning tree (80 characters maximum).

Defaults none

Command Modes SPANNING TREE (The prompt is "config-rstp".)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.7.1.0	Introduced.

Related Commands protocol spanning-tree rstp — enters SPANNING TREE mode on the switch.

disable

Disable RSTP globally on the system.

C9000 Series

Syntax `disable`

To enable Rapid Spanning Tree Protocol, use the `no disable` command.

Defaults RSTP is disabled.

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands protocol spanning-tree rstp — enters SPANNING TREE mode on the switch.

forward-delay

Configure the amount of time the interface waits in the Listening State and the Learning State before transitioning to the Forwarding State.

C9000 Series

Syntax `forward-delay` *seconds*

To return to the default setting, use the `no forward-delay` command.

Parameters

seconds	Enter the number of seconds that the system waits before transitioning RSTP to the forwarding state. The range is from 4 to 30. The default is **15 seconds**.

Defaults **15 seconds**

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands hello-time — changes the time interval between BPDUs.

max-age — changes the wait time before RSTP refreshes the protocol configuration information.

hello-time

Set the time interval between the generation of the RSTP bridge protocol data units (BPDUs).

C9000 Series

Syntax `hello-time [milli-second] seconds`

To return to the default value, use the `no hello-time` command.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10 seconds. The default is **2 seconds**.
milli-second	Enter the keywords `milli-second` to configure a hello time on the order of milliseconds. The range is from 50 to 950 milliseconds

Defaults **2 seconds**

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the `milli-second` option to the S-Series.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The hello time is encoded in BPDUs in increments of 1/256ths of a second. The standard minimum hello time in seconds is 1 second, which is encoded as 256. Millisecond hello times are encoded using values less than 256; the millisecond hello time equals (x/1000)*256.

When you configure millisecond hellos, the default hello interval of 2 seconds is still used for edge ports; the millisecond hello interval is not used.

Related Commands

forward-delay — changes the wait time before RSTP transitions to the Forwarding state.

max-age — changes the wait time before RSTP refreshes the protocol configuration information.

max-age

To maintain configuration information before refreshing that information, set the time interval for the RSTP bridge.

C9000 Series

Syntax

`max-age` *`seconds`*

To return to the default values, use the `no max-age` command.

Parameters

max-age	Enter a number of seconds that the system waits before refreshing configuration information. The range is from 6 to 40 seconds. The default is **20 seconds**.

Defaults

20 seconds

Command Modes

CONFIGURATION RSTP (conf-rstp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

forward-delay — changes the wait time before RSTP transitions to the Forwarding state.

hello-time — changes the time interval between BPDUs.

protocol spanning-tree rstp

To configure RSTP, enter RSTP mode.

C9000 Series

Syntax

```
protocol spanning-tree rstp
```

To exit RSTP mode, use the `exit` command.

Defaults

Not configured

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information RSTP is not enabled when you enter RSTP mode. To enable RSTP globally on the system, use the `no disable` command from RSTP mode.

Example

```
Dell(conf)#protocol spanning-tree rstp
Dell(config-rstp)##no disable
```

Related Commands disable — disables RSTP globally on the system.

show config

View the current configuration for the mode. Only non-default values are displayed.

C9000 Series

Syntax `show config`

Command Modes CONFIGURATION RSTP (conf-rstp)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(conf-rstp)#show config
!
protocol spanning-tree rstp
  no disable
  bridge-priority 16384
```

show spanning-tree rstp

Display the RSTP configuration.

C9000 Series

Syntax

```
show spanning-tree rstp [brief] [guard]
```

Parameters

brief	(OPTIONAL) Enter the keyword `brief` to view a synopsis of the RSTP configuration information.
guard	(OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on an RSTP interface and the current port state.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Added support for the optional `guard` keyword on the C-Series, S-Series, and E-Series TeraScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	Expanded to display the port error disable state (EDS) caused by loopback BPDU inconsistency.
6.2.1.1	Introduced on the E-Series.

Usage Information

The following describes the `show spanning-tree rstp guard` command shown in the following example.

Field	Description
Interface Name	RSTP interface.
Instance	RSTP instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), disabled (DIS), or shut down (EDS Shut).

Field	Description
Guard Type	Types of STP guard configured (Root, Loop, or BPDU guard)

Example (Brief)

```
Dell#show spanning-tree rstp brief
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 8192, Address 0001.e805.e306
Root Bridge hello time 4, max age 20, forward delay 15
Bridge ID Priority 16384, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15
Interface                              Designated
Name   PortID Prio Cost Sts Cost      Bridge ID      PortID
---------- ------- --- ------- -------------------- --------
Te 2/0 128.418 128 20000 FWD 20000 16384 0001.e801.6aa8 128.418
Te 2/1 128.419 128 20000 FWD 20000 16384 0001.e801.6aa8 128.419
Te 2/8 128.426 128 20000 FWD 20000 8192 0001.e805.e306 128.130
Te 2/9 128.427 128 20000 BLK 20000 8192 0001.e805.e306 128.131

Interface
Name   Role PortID Prio Cost Sts Cost  Link-type Edge
---------- ---- ------- --- ------- --------- ----
Te 2/0 Desg 128.418 128 20000 FWD 20000 P2P     Yes
Te 2/1 Desg 128.419 128 20000 FWD 20000 P2P     Yes
Te 2/8 Root 128.426 128 20000 FWD 20000 P2P     No
Te 2/9 Altr 128.427 128 20000 BLK 20000 P2P     No
Dell#
```

Example (EDS, LBK)

NOTE: "LBK_INC" (bold) means Loopback BPDU Inconsistency.

```
Dell#show spanning-tree rstp br
Executing IEEE compatible Spanning Tree Protocol
Root ID Priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15
Bridge ID Priority 32768, Address 0001.e801.6aa8
We are the root
Configured hello time 2, max age 20, forward delay 15

Interface                            Designated
Name   PortID Prio Cost Sts Cost    Bridge ID PortID
- ---- ------- --- ------- -------------------- --------
Te 0/0 128.257 128 20000 EDS 0 32768 0001.e801.6aa8 128.257
Interface
Name   Role PortID    Prio Cost Sts Cost Link-type Edge
--- ------ -------- ---- ------- --- ------- --------- ----
Te 0/0 ErrDis 128.257 128 20000 EDS 0 P2P No

Dell#show spanning-tree rstp
Root Identifier has priority 32768, Address 0001.e801.6aa8
Root Bridge hello time 2, max age 20, forward delay 15, max hops 0
Bridge Identifier has priority 32768, Address 0001.e801.6aa8
Configured hello time 2, max age 20, forward delay 15, max hops 0
We are the root
Current root has priority 32768, Address 0001.e801.6aa8
Number of topology changes 1, last change occurred 00:00:31 ago on Te 0/0
Port 257 (TenGigabitEthernet 0/0) is LBK_INC Discarding
Port path cost 20000, Port priority 128, Port Identifier 128.257
Designated root has priority 32768, address 0001.e801.6aa8
Designated bridge has priority 32768, address 0001.e801.6aa8
Designated port id is 128.257, designated path cost 0
Number of transitions to forwarding state 1
BPDU : sent 27, received 9
The port is not in the Edge port mode
```

Example (Guard)

```
Dell#show spanning-tree rstp guard
Interface
Name   Instance Sts         Guard type
```

```
--------- -------- ------------------
Te 0/1 0        INCON(Root) Rootguard
Te 0/2 0        FWD         Loopguard
Te 0/3 0        BLK         Bpduguard
```

spanning-tree rstp

Configure an RSTP interface with one of these settings: port cost, edge port with optional bridge port data unit (BPDU) guard, port priority, loop guard, or root guard.

C9000 Series

Syntax

```
spanning-tree rstp {cost port-cost | edge-port [bpduguard [shutdown-on-violation]] | priority priority | {loopguard | rootguard}}
```

Parameters

cost *port-cost*	Enter the keyword `cost` then the port cost value. The range is from 1 to 200000. The defaults are: • 10-Gigabit Ethernet interface = **2000** • Port Channel interface with one 10-Gigabit Ethernet = **2000** • Port Channel with two 10 Gigabit Ethernet = **1800**
edge-port	Enter the keywords `edge-port` to configure the interface as a rapid spanning tree edge port.
bpduguard	(OPTIONAL) Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword `bpduguard` to disable the port when it receives a BPDU.
shutdown-on-violation	(OPTIONAL) Enter the keywords `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.
priority *priority*	Enter keyword `priority` then a value in increments of 16 as the priority. The range is from 0 to 240. The default is **128**.
loopguard	Enter the keyword `loopguard` to enable loop guard on an RSTP port or port-channel interface.
rootguard	Enter the keyword `rootguard` to enable root guard on an RSTP port or port-channel interface.

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Added support for the optional `guard` keyword on the C-Series, S-Series, and E-Series TeraScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced the `hardware shutdown-on-violation` options.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Added the optional bridge port data unit (BPDU) guard.
6.2.1.1	Introduced on the E-Series.

Usage Information

The `BPDU guard` option prevents the port from participating in an active STP topology in case a BPDU appears on a port unintentionally, or is misconfigured, or is subject to a DOS attack. This option places the port into an Error Disable state if a BPDU appears and a message is logged so that the administrator can take corrective action.

NOTE: A port configured as an edge port, on an RSTP switch, immediately transitions to the Forwarding state. Only configure ports connected to end-hosts as edge ports. Consider an edge port similar to a port with a `spanning-tree portfast` enabled.

If you do not enable `shutdown-on-violation`, BPDUs are still sent to the RPM CPU.

You cannot enable STP root guard and loop guard at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message displays: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

Enabling Portfast BPDU guard and loop guard at the same time on a port results in a port that remains in a Blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

On the port extender (PE) ports and on VP-LAGs (LAGs created with PE):

- Spanning-tree with `BPDU guard shutdown-on-violation` is enabled as a default setting.
- No spanning tree command is valid. This command is not visible and issuing this command on VP-LAG ports results in a failure.

Example

```
Dell(conf)#interface tengigabitethernet 2/0
Dell(conf-if-te-2/0)#spanning-tree rstp edge-port
Dell(conf-if-te-2/0)#show config
!
interface TenGigabitEthernet 2/0
  no ip address
  switchport
  spanning-tree rstp edge-port
  no shutdown
Dell#
```

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

C9000 Series

Syntax

`tc-flush-standard`

To disable, use the `no tc-flush-standard` command.

Defaults

Disabled

Command Modes

CONFIGURATION (conf-rstp)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

Usage Information

By default, the system implements an optimized flush mechanism for RSTP. This implementation helps in flushing MAC addresses only when necessary (and less often), allowing for faster convergence during topology changes. However, if a standards-based flush mechanism is needed, you can turn on this *knob* command to enable flushing MAC addresses after receiving every topology change notification.

51

Remote Monitoring (RMON)

Dell Networking operating software remote monitoring (RMON) is based on IEEE standards, providing both 32-bit and 64-bit monitoring and long-term statistics collection.

RMON supports the following RMON groups, as defined in RFC-2819, RFC-3273, RFC-3434, and RFC-4502:

- Ethernet Statistics Table; RFC-2819
- Ethernet Statistics High-Capacity Table; RFC-3273, 64bits
- Ethernet History Control Table; RFC-2819
- Ethernet History Table; RFC-2819
- Ethernet History High-Capacity Table; RFC-3273, 64bits
- Alarm Table; RFC-2819
- High-Capacity Alarm Table (64bits); RFC-3434, 64bits
- Event Table; RFC-2819
- Log Table; RFC-2819
- User History Control Table; RFC-4502
- User History Object Table
- User History Table
- Probe Config

RMON does not support the following statistics:

- etherStatsCollisions
- etherHistoryCollisions
- etherHistoryUtilization

NOTE: Only SNMP GET/GETNEXT access is supported. Configure RMON using the RMON commands. Collected data is lost during a chassis reboot.

Topics:

- rmon alarm
- rmon collection history
- rmon collection statistics
- rmon event
- rmon hc-alarm
- show rmon
- show rmon alarms
- show rmon events
- show rmon hc-alarm
- show rmon history
- show rmon log
- show rmon statistics

rmon alarm

Set an alarm on any MIB object.

C9000 Series

Syntax

`rmon alarm` *`number variable interval`* `{delta | absolute} rising-threshold` *`value event-number`* `falling-threshold` *`value event-number`* `[owner` *`string`*`]`

To disable the alarm, use the `no rmon alarm` *`number`* command.

Parameters

number	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.
variable	Enter the MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3. The object type must be a 32-bit integer.
interval	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is from 5 to 3600 seconds.
delta	Enter the keyword `delta` to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
absolute	Enter the keyword `absolute` to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
rising-threshold *value event-number*	Enter the keywords `rising-threshold` then the value (32 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
falling-threshold *value event-number*	Enter the keywords `falling-threshold` then the value (32 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
owner *string*	(OPTIONAL) Enter the keyword `owner` then the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults

owner

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

rmon collection history

Enable the RMON MIB history group of statistics collection on an interface.

C9000 Series

Syntax

`rmon collection history {controlEntry` *`integer`*`} [owner` *`name`*`] [buckets` *`number`*`] [interval` *`seconds`*`]`

To remove a specified RMON history group of statistics collection, use the `no rmon collection history {controlEntry` *`integer`*`}` command.

Parameters

controlEntry *integer*	Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON group of statistics. The integer value must be a unique index in the RMON history table.
owner *name*	(OPTIONAL) Enter the keyword `owner` then the owner name to record the owner of the RMON group of statistics.
buckets *number*	(OPTIONAL) Enter the keyword `buckets` then the number of buckets for the RMON collection history group of statistics. The bucket range is from 1 to 1000. The default is **50**.
interval *seconds*	(OPTIONAL) Enter the keyword `interval` then the number of seconds in each polling cycle. The range is from 5 to 3600 seconds. The default is **1800 seconds**.

Defaults

none

Command Modes

CONFIGURATION INTERFACE (config-if)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

rmon collection statistics

Enable RMON MIB statistics collection on an interface.

C9000 Series

Syntax

`rmon collection statistics {controlEntry` *`integer`*`} [owner` *`name`*`]`

To remove RMON MIB statistics collection on an interface, use the `no rmon collection statistics {controlEntry` *`integer`*`}` command.

Parameters

controlEntry *integer*	Enter the keyword `controlEntry` to specify the RMON group of statistics using a value. Then enter an integer value from 1 to 65535 that identifies the RMON Statistic Table. The integer value must be a unique in the RMON statistic table.
owner *name*	(OPTIONAL) Enter the keyword `owner` then the owner name to record the owner of the RMON group of statistics.

Defaults

none

Command Modes

CONFIGURATION INTERFACE (config-if)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

rmon event

Add an event in the RMON event table.

C9000 Series

Syntax

`rmon event` *`number`* `[log] [trap` *`community`*`] [description` *`string`*`] [owner name]`

To disable RMON on an interface, use the `no rmon event` *`number`* `[log] [trap` *`community`*`] [description` *`string`*`]` command.

Parameters

number	Assign an event number in integer format from 1 to 65535. The number value must be unique in the RMON event table.
log	(OPTIONAL) Enter the keyword `log` to generate an RMON log entry. The log entry is triggered and sets the eventType in the RMON MIB to log or log-and-trap. The default is **No log**.
trap *community*	(OPTIONAL) Enter the keyword `trap` then an SNMP community string to configure the eventType setting in the RMON MIB. This keyword sets either snmp-trap or log-and-trap. The default is **public**.
description *string*	(OPTIONAL) Enter the keyword `description` then a string describing the event.
owner *name*	(OPTIONAL) Enter the keyword `owner` then the name of the owner of this event.

Defaults

As noted in the *Parameters* section.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

rmon hc-alarm

Set an alarm on any MIB object.

C9000 Series

Syntax

`rmon hc-alarm` *`number`* `variable` *`interval`* `{delta | absolute} rising-threshold value` *`event-number`* `falling-threshold` *`value event-number`* `[owner` *`string`*`]`

To disable the alarm, use the `no rmon hc-alarm` *`number`* command.

Parameters

number	Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.
variable	The MIB object to monitor. The variable must be in the SNMP OID format; for example, 1.3.6.1.2.1.1.3 The object type must be a 64-bit integer.
interval	Time, in seconds, the alarm monitors the MIB variables; this is the alarmSampleType in the RMON alarm table. The range is from 5 to 3600 seconds.
delta	Enter the keyword `delta` to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
absolute	Enter the keyword `absolute` to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
rising-threshold *value event-number*	Enter the keywords `rising-threshold` then the value (64 bit) the rising-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the rising threshold exceeds its limit. This value is the same as the alarmRisingEventIndex or alarmTable of the RMON MIB. If there is no corresponding rising-threshold event, the value is zero.
falling-threshold *value event-number*	Enter the keywords `falling-threshold` then the value (64 bit) the falling-threshold alarm is either triggered or reset. Then enter the event-number to trigger when the falling threshold exceeds its limit. This value is the same as the alarmFallingEventIndex or the alarmTable of the RMON MIB. If there is no corresponding falling-threshold event, the value is zero.
owner *string*	(OPTIONAL) Enter the keyword `owner` then the owner name to specify an owner for the alarm. This is the alarmOwner object in the alarmTable of the RMON MIB.

Defaults

owner

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

show rmon

Display the RMON running status including the memory usage.

C9000 Series

Syntax `show rmon`

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell# show rmon
RMON status
  total memory used 218840 bytes.
  ether statistics table: 8 entries, 4608 bytes
  ether history table: 8 entries, 6000 bytes
  alarm table: 390 entries, 102960 bytes
  high-capacity alarm table: 5 entries, 1680 bytes
  event table: 500 entries, 206000 bytes
  log table: 2 entries, 552 bytes
Dell#
```

show rmon alarms

Display the contents of the RMON alarm table.

C9000 Series

Syntax

```
show rmon alarms [index] [brief]
```

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON alarm table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon alarm 1
RMON alarm entry 1
  sample Interval: 5
  object: 1.3.6.1.2.1.1.3
  sample type: absolute value.
  value: 255161
  alarm type: rising or falling alarm.
  rising threshold: 1, RMON event index: 1
  falling threshold: 501, RMON event index: 501
  alarm owner: 1
  alarm status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon alarms brief
Index   SampleType    SNMP OID
-----------------------------------------------------------------------
1       delta         1.3.6.1.2.1.2.2.1.4.1048581
```

show rmon events

Display the contents of the RMON event table.

C9000 Series

Syntax

```
show rmon events [index] [brief]
```

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON event table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon event 1
RMON event entry 1
  description: 1
  event type: LOG and SNMP TRAP.
  event community: public
  event last time sent: none
  event owner: 1
  event status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon events brief
index   eventType            description
-------------------------------------------------------------------
1       LOG and SNMP TRAP    "DELTA RISING LOG TRAP"
2       LOG and SNMP TRAP    "DELTA FALLING LOG TRAP"
```

show rmon hc-alarm

Display the contents of RMON High-Capacity alarm table.

C9000 Series

Syntax `show rmon hc-alarm [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON High-Capacity alarm table in an easy-to-read format.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon hc-alarm 1
RMON high-capacity alarm entry 1
  object: 1.3.6.1.2.1.1.3
  sample interval: 5
  sample type: absolute value.
  value: 185638
  alarm type: rising or falling alarm.
  alarm rising threshold value: positive.
  rising threshold: 1001, RMON event index: 1
  alarm falling threshold value: positive.
  falling threshold: 999, RMON event index: 6
  alarm sampling failed 0 times.
  alarm owner: 1
  alarm storage type: non-volatile.
  alarm status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon hc-alarm brief
index      SNMP OID
```

```
---------------------------------
1          1.3.6.1.2.1.1.3
2          1.3.6.1.2.1.1.3
3          1.3.6.1.2.1.1.3
4          1.3.6.1.2.1.1.3
5          1.3.6.1.2.1.1.3
Dell#
```

show rmon history

Display the contents of the RMON Ethernet history table.

C9000 Series

Syntax `show rmon history [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet history table in an easy-to-read format

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon history 6001
RMON history control entry 6001
  interface: ifIndex.100974631 TenGigabitEthernet 2/0
  bucket requested: 1
  bucket granted: 1
  sampling interval: 5 sec
  owner: 1
  status: OK
Dell#
```

Example (Brief)

```
Dell#show rmon history brief
index    ifIndex      interface
---------------------------------------
6001    100974631    TenGigabitEthernet 1/0
6002    100974631    TenGigabitEthernet 1/0
6003    101236775    TenGigabitEthernet 1/1
6004    101236775    TenGigabitEthernet 1/1
9001    134529054    TenGigabitEthernet 2/0
9002    134529054    TenGigabitEthernet 2/0
9003    134791198    TenGigabitEthernet 2/1
9004    134791198    TenGigabitEthernet 2/1
Dell#
```

show rmon log

Display the contents of the RMON log table.

C9000 Series

Syntax `show rmon log [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON log table in an easy-to-read format.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The log table has a maximum of 500 entries. If the log exceeds that maximum, the oldest log entry is purged to allow room for the new entry.

Example (Index)

```
Dell#show rmon log 2
RMON log entry, alarm table index 2, log index 1
  log time: 14638 (THU AUG 12 22:10:40 2004)
```

```
  description: 2
Dell#
```

Example (Brief)

```
Dell#show rmon logs brief
eventIndex   logIndex     description
--------------------------------------------------------------------------
1             1           "DELTA RISING LOG TRAP"
2             1           "DELTA FALLING LOG TRAP"
2             2           "DELTA FALLING LOG TRAP"
```

show rmon statistics

Display the contents of RMON Ethernet statistics table.

C9000 Series

Syntax

```
show rmon statistics [index] [brief]
```

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword `brief` to display the RMON Ethernet statistics table in an easy-to-read format.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon statistics 6001
RMON statistics entry 6001
  interface: ifIndex.100974631 TengigabitEthernet 2/0
  packets dropped: 0
  bytes received: 0
  packets received: 0
  broadcast packets: 0
  multicast packets: 0
  CRC error: 0
```

```
  under-size packets: 0
  over-size packets: 0
  fragment errors: 0
  jabber errors: 0
  collision: 0
  64bytes packets: 0
  65-127 bytes packets: 0
  128-255 bytes packets: 0
  256-511 bytes packets: 0
  512-1023 bytes packets: 0
  1024-1518 bytes packets: 0
  owner: 1
  status: OK
  <high-capacity data>
  HC packets received overflow: 0
  HC packets received: 0
  HC bytes received overflow: 0
  HC bytes received: 0
  HC 64bytes packets overflow: 0
  HC 64bytes packets: 0
  HC 65-127 bytes packets overflow: 0
  HC 65-127 bytes packets: 0
  HC 128-255 bytes packets overflow: 0
  HC 128-255 bytes packets: 0
  HC 256-511 bytes packets overflow: 0
  HC 256-511 bytes packets: 0
  HC 512-1023 bytes packets overflow: 0
  HC 512-1023 bytes packets: 0
  HC 1024-1518 bytes packets overflow: 0
  HC 1024-1518 bytes packets: 0
Dell#
```

Example (Brief)

```
Dell#show rmon statistics br
index    ifIndex    interface
-----------------------------------------------
6001    100974631    TengigabitEthernet 2/0
6002    100974631    TengigabitEthernet 2/0
6003    101236775    TengigabitEthernet 2/1
6004    101236775    TengigabitEthernet 2/1
9001    134529054    TengigabitEthernet 3/0
9002    134529054    TengigabitEthernet 3/0
9003    134791198    TengigabitEthernet 3/1
9004    134791198    TengigabitEthernet 3/1
Dell#
```

52

Routing Information Protocol (RIP)

Routing information protocol (RIP) is a distance vector routing protocol. The Dell Networking operating software supports both RIP version 1 (RIPv1) and RIP version 2 (RIPv2).

The implementation of RIP is based on IETF RFCs 2453 and RFC 1058. For more information about configuring RIP, refer to the *Dell Networking OS Configuration Guide*.

Topics:

- auto-summary
- clear ip rip
- debug ip rip
- default-information originate
- default-metric
- description
- distance
- distribute-list in
- distribute-list out
- ip poison-reverse
- ip rip receive version
- ip rip send version
- ip split-horizon
- maximum-paths
- neighbor
- network
- offset-list
- output-delay
- passive-interface
- redistribute
- redistribute isis
- redistribute ospf
- router rip
- show config
- show ip rip database
- show running-config rip
- timers basic
- version

auto-summary

Restore the default behavior of automatic summarization of subnet routes into network routes. This command applies only to RIP version 2.

C9000 Series

Syntax `auto-summary`

To send sub-prefix routing information, use the `no auto-summary` command.

Defaults Enabled.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9.(0.0)	Introduced on the C9010.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
pre-6.2.1.1	Introduced on the E-Series.

clear ip rip

Update all the RIP routes in the system routing table.

C9000 Series

Syntax `clear ip rip`

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information This command triggers updates of the main RIP routing tables.

debug ip rip

Examine RIP routing information for troubleshooting.

C9000 Series

Syntax `debug ip rip [interface | database | events [interface] | packet[interface] | trigger]`

To turn off debugging output, use the `no debug ip rip` command.

Parameters

interface	(OPTIONAL) Enter the interface type and ID as one of the following: • For a Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information. • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.
database	(OPTIONAL) Enter the keyword `database` to display messages when there is a change to the RIP database.
events	(OPTIONAL) Enter the keyword `events` to debug only RIP protocol changes.
packet	(OPTIONAL) Enter the keyword `packet` to debug only RIP protocol packet.
trigger	(OPTIONAL) Enter the keyword `trigger` to debug only RIP trigger extensions.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

default-information originate

Generate a default route for the RIP traffic.

C9000 Series

Syntax

`default-information originate [always] [metric` *`metric-value`*`] [route-map` *`map-name`*`]`

To return to the default values, use the `no default-information originate` command.

Parameters

always	(OPTIONAL) Enter the keyword `always` to enable the switch software to always advertise the default route.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number as the metric value. The range is from 1 to 16. The default is **1**.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route-map.

Defaults

Disabled. Metric: **1**.

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information The default route must be present in the switch routing table for the `default-information originate` command to take effect.

default-metric

Change the default metric for routes. To ensure that all redistributed routes use the same metric value, use this command with the `redistribute` command.

C9000 Series

Syntax `default-metric` *number*

To return the default metric to the original values, use the `no default-metric` command.

Parameters

number	Specify a number. The range is from 1 to 16. The default is **1**.

Defaults **1**

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information	This command ensures that route information being redistributed is converted to the same metric value.
Related Commands	redistribute — allows you to redistribute routes learned by other methods.

description

Enter a description of the RIP routing protocol.

C9000 Series

Syntax	`description {description}` To remove the description, use the `no description {description}` command.
Parameters	***description*** Enter a description to identify the RIP protocol (80 characters maximum).
Defaults	none
Command Modes	ROUTER RIP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.7.1.0	Introduced on the E-Series.

Related Commands	router rip — enters ROUTER mode on the switch.

distance

Assign a weight (for prioritization) to all routes in the RIP routing table or to a specific route. Lower weights ("administrative distance") are preferred.

C9000 Series

Syntax	`distance weight [ip-address mask [prefix-name]]`

To return to the default values, use the `no distance weight [ip-address mask]` command.

Parameters

weight	Enter a number from 1 to 255 for the weight (for prioritization). The default is **120**.
ip-address	(OPTIONAL) Enter the IP address, in dotted decimal format (A.B.C.D), of the host or network to receive the new distance metric.
mask	If you enter an IP address, also enter a mask for that IP address, in either dotted decimal format or /prefix format (/x).
prefix-name	(OPTIONAL) Enter a configured prefix list name.

Defaults weight = **120**

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands default-metric — assigns one distance metric to all routes learned using the `redistribute` command.

distribute-list in

Configure a filter for incoming routing updates.

C9000 Series

Syntax `distribute-list prefix-list-name in [interface]`

To delete the filter, use the `no distribute-list prefix-list-name in` command.

Parameters

prefix-list-name	Enter the name of a configured prefix list.
interface	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096.

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.29.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands ip prefix-list — enters PREFIX-LIST mode and configures a prefix list.

distribute-list out

Configure a filter for outgoing routing updates.

C9000 Series

Syntax `distribute-list prefix-list-name out [interface | bgp | connected | ospf | static]`

To delete the filter, use the `no distribute-list prefix-list-name out` command.

Parameters

prefix-list-name Enter the name of a configured prefix list.

interface (OPTIONAL) Identifies the interface type slot/port as one of the following:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

connected	(OPTIONAL) Enter the keyword `connected` to filter only directly connected routes.
ospf	(OPTIONAL) Enter the keyword `ospf` to filter all OSPF routes.
static	(OPTIONAL) Enter the keyword `static` to filter manually configured routes.

Defaults Not configured.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands ip prefix-list — enters PREFIX-LIST mode and configures a prefix list.

ip poison-reverse

Set the prefix of the RIP routing updates to the RIP infinity value.

C9000 Series

Syntax `ip poison-reverse`

To disable poison reverse, use the `no ip poison-reverse` command.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands ip split-horizon — sets the RIP routing updates to exclude routing prefixes.

ip rip receive version

To receive specific versions of RIP, set the interface. The RIP version you set on the interface overrides the version command in ROUTER RIP mode.

C9000 Series

Syntax

```
ip rip receive version [1] [2]
```

To return to the default, use the `no ip rip receive version` command.

Parameters

1	(OPTIONAL) Enter the number `1` for RIP version 1.
2	(OPTIONAL) Enter the number `2` for RIP version 2.

Defaults **RIPv1** and **RIPv2**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.

Version	Description
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information If you want the interface to receive both versions of RIP, use the `ip rip receive version 1 2` command.

Related Commands ip rip send version — sets the RIP version for sending RIP traffic on an interface.

version — sets the RIP version the switch software uses.

ip rip send version

To send a specific version of RIP, set the interface. The version you set on the interface overrides the version command in ROUTER RIP mode.

C9000 Series

Syntax `ip rip send version [1] [2]`

To return to the default value, use the `no ip rip send version` command.

Parameters

1	(OPTIONAL) Enter the number `1` for RIP version 1. The default is RIPv1.
2	(OPTIONAL) Enter the number `2` for RIP version 2.

Defaults **RIPv1**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information To enable the interface to send both version of RIP packets, use the `ip rip send version 1 2` command.

Related Commands ip rip receive version — sets the RIP version for the interface to receive traffic.

version — sets the RIP version for the switch software.

ip split-horizon

Enable split-horizon for RIP data on the interface. As described in RFC 2453, the split-horizon scheme prevents any routes learned over a specific interface to be sent back out that interface.

C9000 Series

Syntax `ip split-horizon`

To disable split-horizon, use the `no ip split-horizon` command.

Defaults Enabled

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands ip poison-reverse — sets the prefix for RIP routing updates.

maximum-paths

Set RIP to forward packets over multiple paths.

C9000 Series

Syntax `maximum-paths` *number*

To return to the default values, use the `no maximum-paths` commands.

Parameters

number	Enter the number of paths. The range is from 1 to 16. The default is **4** paths.

Defaults **4**

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information RIP supports a maximum of 16 ECMP paths.

neighbor

Define a neighbor router with which to exchange RIP information.

C9000 Series

Syntax `neighbor ip-address`

To delete a neighbor setting, use the `no neighbor ip-address` command.

Parameters

ip-address	Enter the IP address, in dotted decimal format, of a router with which to exchange information.

Defaults Not configured.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

When a neighbor router is identified, unicast data exchanges occur. Multiple neighbor routers are possible.

To ensure that only specific interfaces are receiving and sending data, use the `passive-interface` command with the `neighbor` command.

Related Commands

passive-interface — sets the interface to only listen to RIP broadcasts.

network

Enable RIP for a specified network. To enable RIP on all networks connected to the switch, use this command.

C9000 Series

Syntax

`network` *`ip-address`*

To disable RIP for a network, use the `no network` *`ip-address`* command.

Parameters

ip-address	Specify an IP network address in dotted decimal format. You cannot specify a subnet.

Defaults

No RIP network is configured.

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

You can enable an unlimited number of RIP networks.

RIP operates over interfaces configured with any address the `network` command specifies.

offset-list

Specify a number to add to the incoming or outgoing route metrics learned using RIP.

C9000 Series

Syntax

`offset-list` *`prefix-list-name`* `{in | out}` *`offset`* `[`*`interface`*`]`

To delete an offset list, use the `no offset-list` *`prefix-list-name`* `{in | out}` *`offset`* `[`*`interface`*`]` command.

Parameters

prefix-list-name	Enter the name of an established Prefix list to determine which incoming routes are modified.
offset	Enter a number from zero (0) to 16 to be applied to the incoming route metric matching the access list specified. If you set an offset value to zero (0), no action is taken.
interface	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information When the offset metric is applied to an interface, that value takes precedence over an offset value that is not extended to an interface.

Related Commands ip prefix-list — enters PREFIX-LIST mode and configure a prefix list.

output-delay

Set the interpacket delay of successive packets to the same neighbor.

C9000 Series

Syntax `output-delay` *delay*

To return to the switch software defaults for interpacket delay, use the `no output-delay` command.

Parameters

delay	Specify a number of milliseconds as the delay interval. The range is from 8 to 50.

Defaults Not configured.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information This command is intended for low-speed interfaces.

passive-interface

Suppress routing updates on a specified interface.

C9000 Series

Syntax `passive-interface` *interface*

To delete a passive interface, use the `no passive-interface` *interface* command.

Parameters

interface Enter the following information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 4096.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a VLAN, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information Although the passive interface does not send or receive routing updates, the network on that interface still includes in RIP updates sent using other interfaces.

Related Commands neighbor — enables RIP for a specified network.

network — defines a neighbor.

redistribute

Redistribute information from other routing instances.

C9000 Series

Syntax

```
redistribute {connected | static}
```

To disable redistribution, use the no redistribute {connected | static} command.

Parameters

connected	Enter the keyword `connected` to specify that information from active routes on interfaces is redistributed.
static	Enter the keyword `static` to specify that information from static routes is redistributed.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.

Related Commands

default-information originate — generates a default route for RIP traffic.

redistribute isis

Redistribute routing information from an IS-IS instance.

C9000 Series

Syntax

`redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value] [route-map map-name]`

To disable redistribution, use the `no redistribute isis [tag] [level-1 | level-1-2 | level-2] [metric metric-value] [route-map map-name]` command.

Parameters

tag	(OPTIONAL) Enter the name of the IS-IS routing process.
level-1	(OPTIONAL) Enter the keywords `level-1` to redistribute only IS-IS Level-1 routes.
level-1-2	(OPTIONAL) Enter the keywords `level-1-2` to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keywords `level-2` to redistribute only IS-IS Level-2 routes.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number as the metric value. The range is from 0 to 16.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
6.2.1.1	Introduced on the E-Series.

redistribute ospf

Redistribute routing information from an OSPF process.

C9000 Series

Syntax

`redistribute ospf` *process-id* `[match external {1 | 2} | match internal | metric` *metric-value*`] [route-map` *map-name*`]`

To disable redistribution, use the `no redistribute ospf` *process-id* `[match external {1 | 2} | match internal | metric` *metric-value*`] [route-map` *map-name*`]` command.

Parameters

process-id	Enter a number that corresponds to the OSPF process ID to redistribute. The range is from 1 to 65355.
match external {1 | 2}	(OPTIONAL) Enter the keywords `match external` then the numbers `1` or `2` to indicated that external 1 routes or external 2 routes should be redistributed.
match internal	(OPTIONAL) Enter the keywords `match internal` to indicate that internal routes should be redistributed.
metric *metric-value*	(OPTIONAL) Enter the keyword `metric` then a number as the metric value. The range is from 0 to 16.
route-map *map-name*	(OPTIONAL) Enter the keywords `route-map` then the name of a configured route map.

Defaults

Not configured.

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

router rip

To configure and enable RIP, enter ROUTER RIP mode.

C9000 Series

Syntax

`router rip`

To disable RIP, use the `no router rip` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

To enable RIP, assign a network address using the `network` command.

Example

```
Dell(conf)#router rip
Dell(conf-router_rip)#
```

Related Commands

network — enables RIP.

exit — returns to CONFIGURATION mode.

show config

Display the changes you made to the RIP configuration. The default values are not shown.

C9000 Series

Syntax `show config`

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(conf-router_rip)#show config
!
router rip
  network 172.31.0.0
  passive-interface TenGigabitEthernet 0/1
Dell(conf-router_rip)#
```

show ip rip database

Display the routes that RIP learns. If the switch learned no RIP routes, no output is generated.

C9000 Series

Syntax `show ip rip database [ip-address mask]`

Parameters

ip-address	(OPTIONAL) Specify an IP address in dotted decimal format to view RIP information on that network only. If you enter an IP address, also enter a mask for that IP address.
mask	(OPTIONAL) Specify a mask, in /network format, for the IP address.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information The following describes the `show ip rip database` command shown in the following example.

Field	Description
Total number of routes in RIP database	Displays the number of RIP routes stored in the RIP database.
100.10.10.0/24 directly connected	Lists the routes directly connected.
150.100.0.0 redistributed	Lists the routes learned through redistribution.
209.9.16.0/24...	Lists the routes and the sources advertising those routes.

Example

```
Dell#show ip rip database
Total number of routes in RIP database: 1624
204.250.54.0/24
      [50/1] via 192.14.1.3, 00:00:12, TenGigabitEthernet 0/15
204.250.54.0/24     auto-summary
203.250.49.0/24
      [50/1] via 192.13.1.3, 00:00:12, TenGigabitEthernet 0/14
203.250.49.0/24     auto-summary
210.250.40.0/24
      [50/2] via 1.1.18.2, 00:00:14, Vlan 18
      [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
210.250.40.0/24     auto-summary
207.250.53.0/24
      [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
      [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
      [50/2] via 1.1.10.2, 00:00:18, Vlan 10
207.250.53.0/24     auto-summary
208.250.42.0/24
      [50/2] via 1.1.120.2, 00:00:55, Port-channel 20
      [50/2] via 1.1.130.2, 00:00:12, Port-channel 30
      [50/2] via 1.1.10.2, 00:00:18, Vlan 10
208.250.42.0/24     auto-summary
```

show running-config rip

Display the current RIP configuration.

C9000 Series

Syntax `show running-config rip`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series.
7.6.1.0	Introduced on the E-Series.

Example

```
show running-config rip
!
router rip
  distribute-list Test1 in
  distribute-list Test21 out
  network 10.0.0.0
  passive-interface TenGigabitEthernet 2/0
  neighbor 20.20.20.20
  redistribute ospf 999
  version 2
```

timers basic

Manipulate the RIP timers for routing updates, invalid, holddown times, and flush time.

C9000 Series

Syntax `timers basic update` *`invalid holddown flush`*

To return to the default settings, use the `no timers basic` command.

Parameters

update	Enter the number of seconds to specify the rate at which RIP routing updates are sent. The range is from zero (0) to 4294967295. The default is **30 seconds**.
invalid	Enter the number of seconds to specify the time interval before routing updates are declared invalid or expired. The invalid value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is **180 seconds**.
holddown	Enter the number of seconds to specify a time interval during which the route is marked as unreachable but still sending RIP packets. The holddown value should be at least three times the update timer value. The range is from zero (0) to 4294967295. The default is **180 seconds**.
flush	Enter the number of seconds to specify the time interval during which the route is advertised as unreachable. When this interval expires, the route is flushed from the routing table. The flush value should be greater than the update value. The range is from zero (0) to 4294967295. The default is **240 seconds**.

Defaults

- update = **30 seconds**
- invalid = **180 seconds**
- holddown = **180 seconds**
- flush = **240 seconds**

Command Modes ROUTER RIP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information If you change the timers on one router, also synchronize the timers on all routers in the RIP domain.

version

Specify either RIP version 1 or RIP version 2.

C9000 Series

Syntax

```
version {1 | 2}
```

To return to the default version setting, use the `no version` command.

Parameters

1	Enter the keyword `1` to specify RIP version 1.
2	Enter the keyword `2` to specify RIP version 2.

Defaults

The system sends RIPv1 and receives RIPv1 and RIPv2.

Command Modes

ROUTER RIP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

ip rip receive version — sets the RIP version the interface receives.

ip rip send version — sets the RIP version the interface sends.

53

Security

This chapter contains various types of security commands offered in the Dell Networking operating software.
The commands are listed in the following sections:

- AAA Accounting Commands
- Authorization and Privilege Commands
- Obscure Password Command
- Authentication and Password Commands
- RADIUS Commands
- TACACS+ Commands
- Port Authentication (802.1X) Commands
- SSH Server and SCP Commands
- Secure DHCP Commands

For configuration details, refer to the Security chapter in the *Dell Networking OS Configuration Guide*.

NOTE: Starting with the Dell Networking OS version 7.2.1.0, LEAP with MSCHAP v2 supplicant is implemented.

Topics:

- Role-Based Access Control Commands
- AAA Accounting Commands
- Authorization and Privilege Commands
- Authentication and Password Commands
- RADIUS Commands
- TACACS+ Commands
- Port Authentication (802.1X) Commands
- SSH Server and SCP Commands
- Secure DHCP Commands
- ICMP Vulnerabilities
- System Security Commands

Role-Based Access Control Commands

With Role-Based Access Control (RBAC), access and authorization is controlled based on a user's role. Users are granted permissions based on their user roles, not on their individual user ID. User roles are created for job functions and through those roles they acquire the permissions to perform their associated job function.

This section describes the syntax and usage of RBAC-specific commands. You can find information on other related security commands in this chapter:

- aaa accounting
- aaa authentication login
- aaa authorization commands
- authorization

- show accounting
- show users
- username

aaa authorization role-only

Configure authentication to use the user's role only when determining if access to commands is permitted.

C9000

Syntax

`aaa authorization role-only`

To return to the default setting, use the `no aaa authentication role-only` command.

Parameters

name	Enter a text string for the name of the user up to 63 characters. It cannot be one of the system defined roles (sysadmin, secadmin, netadmin, netoperator).
inherit *existing-role-name*	Enter the `inherit` keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).

Defaults

none

Command Modes

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information

By default, access to commands are determined by the user's role (if defined) or by the user's privilege level. If the `aaa authorization role-only` command is enabled, then only the user's role is used.

Before you enable role-based only AAA authorization:

1. Locally define a system administrator user role.This will give you access to login with full permissions even if network connectivity to remote authentication servers is not available.
2. Configure login authentication on the console. This ensures that all users are properly identified through authentication no matter the access point
3. Specify an authentication method (RADIUS, TACACS+, or Local).
4. Specify authorization method (RADIUS, TACACS+ or Local).
5. Verify the configuration has been applied to the console or VTY line.

role

Changes command permissions for roles.

C9000

Syntax

`role mode` { { { `addrole` | `deleterole` } *role-name* } | `reset` } *command*

To delete access to a command, use the `no role` *mode role-name*

Parameters

mode	Enter one of the following keywords as the mode for which you are controlling access: configure for CONFIGURATION mode exec for EXEC mode interface for INTERFACE modes line for LINE mode route-map for Route-map mode router for Router mode
addrole	Enter the keyword `addrole` to add permission to the command. You cannot add or delete rights for the sysadmin role.
deleterole	Enter the keyword deleterole to remove access to the command. You cannot add or delete rights for the sysadmin role.
role-name	Enter a text string for the name of the user role up to 63 characters. These are 3 system defined roles you can modify: secadmin, netadmin, and netoperator.
reset	Enter the keyword `reset` to reset all roles back to default for that command.
command	Enter the command's keywords to assign the command to a certain access level. You can enter one or more keywords.

Defaults

none

Command Modes

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

show role

Display information on permissions assigned to a command, including user role and/or permission level.

C9000

Syntax `show role mode {mode} {command}`

Parameters

command	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.
mode *mode*	Enter keyword then one of the following modes. • configure • exec • interface • line • route-map • router

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL

Examples

```
Dell#show role mode configure username
Role access: sysadmin

Dell#show role mode configure management route
Role access: netadmin, sysadmin

Dell#show role mode configure management crypto-policy
Role access: secadmin, sysadmin
```

show userroles

Display information on all defined user roles.

C9000

Syntax `show userroles`

Command Modes EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL.

Example

```
Dell#show userroles
Role          Inheritance  Modes
netoperator                Exec
netadmin                   Exec Config Interface Line Router IP
                           Route-map Protocol MAC
secadmin                   Exec Config
sysadmin                   Exec Config Interface Line Router IP
                           Route-map Protocol MAC
netoperator
testadmin     netadmin     Exec Config Interface Line Router IP
                           Route-map Protocol MAC
```

userrole

Create user roles for the role-based security model.

C9000

Syntax

`userrole` *`name`* `inherit` *`existing-role-name`*

To delete a role name, use the no userrole *name* command. Note that the reserved role names may not be deleted.

Parameters

name	Enter a text string for the name of the user up to 63 characters. It cannot be one of the system defined roles (sysadmin, secadmin, netadmin, netoperator).
inherit *existing-role-name*	Enter the `inherit` keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).

Defaults

none

Command Modes

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL.

Usage Information

Instead of using the system defined user roles, you can create a new user role that best matches your organization. When you create a new user role, you first inherit permissions from one of the system defined roles. Otherwise you would have to create a user role from scratch. You then restrict commands or add commands to that role. For information about this topic, See *Modifying Command Permissions for Roles*.

NOTE: You can change user role permissions on system pre-defined user roles or user-defined user roles.

Important Points to Remember

Consider the following when creating a user role:

- Only the system administrator and user-defined roles inherited from the system administrator can create roles and usernames. Only the system administrator, security administrator, and roles inherited from these can use the `role` command to modify command permissions. The security administrator and roles inherited by security administrator can only modify permissions for commands they already have access to.
- Make sure you select the correct role you want to inherit.

NOTE: If you inherit a user role, you cannot modify or delete the inheritance. If you want to change or remove the inheritance, delete the user role and create it again. If the user role is in use, you cannot delete the user role.

AAA Accounting Commands

AAA Accounting enables tracking of services that users are accessing and the amount of network resources being consumed by those services. When you enable AAA Accounting, the network server reports user activity to the TACACS+ security server in the form of accounting records. Each accounting record is comprised of accounting AV pairs and is stored on the access control server.

As with authentication and authorization, you must configure AAA Accounting by defining a named list of accounting methods, and then applying that list to various interfaces.

aaa accounting

Enable AAA Accounting and create a record for monitoring the accounting function.

C9000 Series

Syntax

`aaa accounting {commands {`*`level`*` | role `*`role-name`*` | dot1x | exec | rest | suppress | system} {`*`name`*` | default} {start-stop | wait-start | stop-only} {radius | tacacs+}`

To disable AAA Accounting, use the `no aaa accounting {commands {`*`level`*` | role `*`role-name`*` | dot1x | exec | rest | suppress | system} {`*`name`*` | default} {start-stop | wait-start | stop-only} {radius | tacacs+}` command.

Parameters

system	Enter the keyword `system` to send accounting information of any other AAA configuration.
exec	Enter the keyword `exec` to send accounting information when a user has logged in to EXEC mode.
dot1x	Enter the keyword `dot1x` to send accounting information when a dot1x user has logged in.
commands {*level* | role *role-name*	Enter the keyword `command` then a privilege level for accounting of commands executed at that privilege level or enter the keyword `role` then the role name for accounting of commands executed by a user with that user role.
dot1x	Enter the keyword `dot1x` for dot1x events.
name | default	Enter one of the following: • For `name`, enter a user-defined name of a list of accounting methods.

- For `default`, the default accounting methods used.

start-stop	Enter the keywords `start-stop` to send a "start accounting" notice at the beginning of the requested event and a "stop accounting" notice at the end of the event.
wait-start	Enter the keywords `wait-start` to ensure that the TACACS+ security server acknowledges the start notice before granting the user's process request.
stop-only	Enter the keywords `stop-only` to instruct the TACACS+ security server to send a "stop record accounting" notice at the end of the requested user process.
radius	Enter the keyword `radius` to use RADIUS service for exec and dot1x accounting.
tacacs+	Enter the keyword `tacacs+` to use TACACS+ service for accounting.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.14(1.5)	Added support for RADIUS accounting.
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, and MXL
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Usage Information The `aaa-accounting dot1x default` command enables the default settings for Authentication, Authorization, and Accounting (AAA) dot1x accounting events. The command is disabled by default.

You can choose the `start-stop`, `stop-only` or the `wait-start` option to manage and monitor the dot1x event messages.

In the example below, TACACS+ accounting is used to track all usage of EXEC command and commands on privilege level 15.

Privilege level 15 is the default. If you want to track usage at privilege level 1 for example, use the `aaa accounting command 1` command. If you want to track usage by role name for the `secadmin`, for example, use `aaa accounting command role secadmin`.

Example

```
Dell(conf)# aaa accounting exec default start-stop tacacs+
Dell(conf)# aaa accounting command 15 default start-stop tacacs+
Dell(conf)# aaa accounting command role secaadmin default start-stop tacacs+
```

Related Commands

enable password — changes the password for the `enable` command.

login authentication — enables AAA login authentication on the terminal lines.

password — creates a password.

tacacs-server host — specifies a TACACS+ server host.

aaa accounting suppress

Prevent the generation of accounting records of users with the user name value of NULL.

C9000 Series

Syntax

```
aaa accounting suppress null-username
```

To permit accounting records to users with user name value of NULL, use the `no aaa accounting suppress null-username` command.

Defaults

Accounting records are recorded for all users.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4280T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Usage Information

The system issues accounting records for all users on the system, including users whose username string, due to protocol translation, is NULL. For example, a user who comes on line with the `aaa authentication login method-list none` command is applied. To prevent the accounting records from being generated for sessions that do not have user names associated to them, use the `aaa accounting suppress` command.

accounting

Apply an accounting method list to terminal lines.

C9000 Series

Syntax `accounting {exec | commands {level | role role-name} method-list`

Parameters

exec	Enter the keyword `exec` to apply an EXEC level accounting method list.
commands {*level* | role *role-name*}	Enter the keywords `commands level` to apply an EXEC and CONFIGURATION level accounting method list by enter the keyword `role` and then the role name for accounting of commands executed by a user with that user role.
method-list	Enter a method list that you defined using the `aaa accounting exec` or `aaa accounting` commands.

Defaults none

Command Modes LINE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Example The following example configures accounting for the role secadmin using default

```
Dell(conf-vty-0)# accounting commands role secadmin default
```

Related Commands aaa accounting — enables AAA Accounting and creates a record for monitoring the accounting function.

show accounting

Display the active accounting sessions for each online user.

C9000 Series

Syntax

```
show accounting
```

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Usage Information

This command steps through all active sessions and then displays the accounting records for the active account functions.

Example

```
Dell#show accounting
Active accounted actions on tty2, User guest Priv 1 Role netoperator
  Task ID 1, EXEC Accounting record, 00:00:30 Elapsed,
service=shell
Active accounted actions on tty3, User admin Priv 15 Role sysadmin
  Task ID 2, EXEC Accounting record, 00:00:26 Elapsed,
service=shell
```

Related Commands

aaa accounting — enables AAA Accounting and creates a record for monitoring the accounting function.

Authorization and Privilege Commands

To set command line authorization and privilege levels, use the following commands.

authorization

Apply an authorization method list to terminal lines.

C9000 Series

Syntax `authorization {exec | commands {level | role role-name}} method-list`

Parameters

exec	Enter the keyword `exec` to apply an EXEC level authorization method list.
commands {*level* | role *role-name*}	Enter the keyword commands followed by either a privilege level for accounting of commands executed at that privilege level, or enter the keyword `role` then the role name for authorization of commands executed by a user with that user role.
method-list	Enter a method list that you defined using the `aaa accounting exec` or `aaa accounting` commands.

Defaults none

Command Modes LINE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Related Commands aaa authorization commands — sets the parameters that restrict (or permit) a user's access to EXEC and CONFIGURATION level commands

aaa authorization exec — sets the parameters that restrict (or permit) a user's access to EXEC level commands.

aaa authorization commands

Set parameters that restrict (or permit) a user's access to EXEC and CONFIGURATION level commands.

C9000 Series

Syntax

`aaa authorization commands {level | role role-name}{name|default} {local | tacacs+| none}`

Undo a configuration with the `no aaa authorization commands {level | role role-name} {name|default} {local | tacacs+ | none}` command.

Parameters

commands *level*	Enter the keyword `commands` then the command privilege level for command level authorization.
role *role-name*	Enter the keyword `role` then the role name.
name	Define a name for the list of authorization methods.
default	Define the default list of authorization methods.
local	Use the authorization parameters on the system to perform authorization.
tacacs+	Use the TACACS+ protocol to perform authorization.
none	Enter the keyword `none` to apply no authorization.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Added support for RADIUS.

aaa authorization config-commands

Set parameters that restrict (or permit) a user's access to EXEC level commands.

C9000 Series

Syntax

`aaa authorization config-commands`

Disable authorization checking for CONFIGURATION level commands using the `no aaa authorization config-commands` command.

Defaults

Enabled when you configure `aaa authorization commands` command.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the E-Series.

Usage Information

By default, the `aaa authorization commands` command configures the system to check both EXEC level and CONFIGURATION level commands. Use the command `no aaa authorization config-commands` to enable only EXEC-level command checking.

aaa authorization exec

Set parameters that restrict (or permit) a user's access to EXEC-level commands.

C9000 Series

Syntax

`aaa authorization exec {`*`name`*` | default} {local || tacacs+ || if-authenticated || none}`

To disable authorization checking for EXEC level commands, use the `no aaa authorization exec` command.

Parameters

name	Define a name for the list of authorization methods.
default	Define the default list of authorization methods.
local	Use the authorization parameters on the system to perform authorization.
tacacs+	Use the TACACS+ protocol to perform authorization.
none	Enter the keyword `none` to apply no authorization.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Added support for RADIUS.

privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

C9000 Series

Syntax `privilege` *`mode`* `{level` *`level command`* `| reset` *`command`*`}`

To delete access to a level and command, use the `no privilege mode level level command` command.

Parameters

mode	Enter one of the following keywords as the mode for which you are controlling access: • `configure` for CONFIGURATION mode • `exec` for EXEC mode • `interface` for INTERFACE modes • `line` for LINE mode • `route-map` for ROUTE-MAP mode • `router` for ROUTER OSPF, ROUTER RIP, ROUTER ISIS and ROUTER BGP modes

	level *level*	Enter the keyword `level` then a number for the access level. The range is from 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes and commands.
	reset	Enter the keyword `reset` to return the security level to the default setting.
	command	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information To define a password for the level to which you are assigning privilege or access, use the `enable password` command.

privilege level (LINE mode)

Change the access level for users on the terminal lines.

C9000 Series

Syntax `privilege level` *`level`*

To delete access to a terminal line, use the `no privilege level` *`level`* command.

Parameters

	level *level*	Enter the keyword `level` then a number for the access level. The range is from 0 to 15. Level 1 is EXEC mode and Level 15 allows access to all CLI modes.

Defaults *level* = **15**

Command Modes LINE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Authentication and Password Commands

To manage access to the system, use the following the commands:

aaa authentication enable

Configure AAA Authentication method lists for user access to EXEC privilege mode (the “Enable” access).

C9000 Series

Syntax

`aaa authentication enable {default | method-list-name} method [... method2]`

To return to the default setting, use the `no aaa authentication enable {default | method-list-name} method [... method2]` command.

Parameters

default	Enter the keyword `default` then the authentication methods to use as the default sequence of methods for the Enable login. The default is `default enable`.
method-list-name	Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at login.
method	Enter one of the following methods: • `enable`: use the password the `enable password` command defines in CONFIGURATION mode. • `line`: use the password the `password` command defines in LINE mode. • `none`: no authentication. • `radius`: use the RADIUS servers configured with the `radius-server host` command.

- `tacacs+`: use the TACACS+ server(s) configured with the `tacacs-server host` command.

... method2	(OPTIONAL) In the event of a "no response" from the first method, the system applies the next configured method.

Defaults Use the `enable` password.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information By default, the `Enable password` is used. If you configure `aaa authentication enable default`, the system uses the methods defined for `Enable access` instead.

Methods configured with the `aaa authentication enable` command are evaluated in the order they are configured. If authentication fails using the primary method, the system employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, the system proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

Related Commands enable password — changes the password for the `enable` command.

login authentication — enables AAA login authentication on the terminal lines.

password — creates a password.

radius-server host — specifies a RADIUS server host.

tacacs-server host — specifies a TACACS+ server host.

aaa authentication login

Configure AAA Authentication method lists for user access to EXEC mode (`Enable log-in`).

C9000 Series

Syntax

`aaa authentication login {method-list-name | default} method [... method4]`

To return to the default setting, use the `no aaa authentication login {method-list-name | default}` command.

Parameters

method-list-name	Enter a text string (up to 16 characters long) as the name of a user-configured method list that can be applied to different lines.
default	Enter the keyword `default` to specify that the method list specified is the default method for all terminal lines.
method	Enter one of the following methods: • `enable`: use the password the `enable password` command defines in CONFIGURATION mode. Not available if role-only is in use. • `line`: use the password the `password` command defines in LINE mode. Not available if role-only is in use. • `local`: use the password for the userid contained in the local password database. • `none`: no authentication. Not available if role-only is in use. • `radius`: use the RADIUS servers configured with the `radius-server host` command. • `tacacs+`: use the TACACS+ servers configured with the `tacacs-server host` command.
... method4	(OPTIONAL) Enter up to four additional methods. In the event of a "no response" from the first method, the system applies the next configured method (up to four configured methods).

Defaults

Not configured (that is, no authentication is performed).

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

By default, the locally configured username password is used. If you configure `aaa authentication login default`, the system uses the methods this command defines for login instead.

Methods configured with the `aaa authentication login` command are evaluated in the order they are configured. If users encounter an error with the first method listed, the system applies the next method configured. If users fail the first method listed, no other methods are applied. The only exception is the local method. If the user's name is not listed in the local database, the next method is applied. If the correct user name/password combination is not entered, the user is not allowed access to the switch.

NOTE: If authentication fails using the primary method, the system employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, the system proceeds to the next authentication method. The TACACS+ is incorrect, but the user is still authenticated by the secondary method.

After configuring the `aaa authentication login` command, configure the `login authentication` command to enable the authentication scheme on terminal lines.

Connections to the SSH server work with the following login mechanisms: local, radius, and tacacs.

Related Commands

login authentication — enables AAA login authentication on the terminal lines.

password — creates a password.

radius-server host — specifies a RADIUS server host.

tacacs-server host — specifies a TACACS+ server host.

aaa reauthenticate enable

Enable re-authentication of user whenever there is a change in the authenticators.

Syntax

```
aaa reauthenticate enable
```

To disable the re-authentication option, use the `no aaa reauthenticate enable` command.

Defaults

Disabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced this command.

Usage Information

When an operating system enables to change the user authenticators, the users might access resources and perform tasks that they do not have authorization.

Once re-authentication is enabled, Dell Networking OS prompts the users to re-authenticate whenever there is a change in authenticators.

The change in authentication happens when:

- Add or remove an authentication server (RADIUS/TACACS+)
- Modify an AAA authentication/authorization list
- Change to role-only (RBAC) mode

The re-authentication is also applicable for authenticated 802.1x devices. When there is a change in the authentication servers, the supplicants connected to all the ports are forced to re-authenticate.

Example

```
Dell(config)#aaa reauthenticate enable
```

```
Dell(config)#aaa authentication login vty_auth_list radius
Force all logged-in users to re-authenticate (y/n)?
```

```
Dell(config)#radius-server host 192.100.0.12
Force all logged-in users to re-authenticate (y/n)?
```

access-class

Restrict incoming connections to a particular IP address in a defined IP access control list (ACL).

C9000 Series

Syntax

`access-class` *`access-list-name`*

To delete a setting, use the `no access-class` command.

Parameters

access-list-name	Enter the name of an established IP Standard ACL.

Defaults

Not configured.

Command Modes

LINE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands

line — applies an authentication method list to the designated terminal lines.

ip access-list standard — names (or selects) a standard access list to filter based on the IP address.

ip access-list extended — names (or selects) an extended access list based on the IP addresses or protocols.

enable password

Change the password for the `enable` command.

C9000 Series

Syntax

`enable password [level level] [encryption-type] password`

To delete a password, use the `no enable password [encryption-type] password [level level]` command.

Parameters

level *level*	(OPTIONAL) Enter the keyword `level` then a number as the level of access. The range is from 1 to 15.
encryption-type	(OPTIONAL) Enter the number `7` or `0` as the encryption type. Enter a `7` then a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults

No password is configured. *level* = **15**.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Neworking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

To control access to command modes, use this command to define a password for a level and use the `privilege level (CONFIGURATION mode)` command.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type "`abcd CNTL v ]e`". When the password is created, you do not use the CNTL + v key combination and enter "`abcd]e`".

NOTE: The question mark (?) and the tilde (~) are not supported characters.

Related Commands

show running-config — views the current configuration.

privilege level (CONFIGURATION mode) — controls access to the command modes within the switch.

enable sha256-password

Configure SHA-256 based password for the `enable` command.

Syntax

`enable sha256-password [level level] [encryption-type] password`

To delete a password, use the `no enable sha256-password [encryption-type] password [level level]` command.

Parameters

sha256-password	Enter the keyword `sha256-password` then the `encryption-type` or the password.
level *level*	(OPTIONAL) Enter the keyword `level` then a number as the level of access. The range is from 1 to 15.
encryption-type	(OPTIONAL) Enter the number `8` or `0` as the encryption type. Enter `8` to enter the sha256–based hashed password.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults

No password is configured. *level* = **15**.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.0)	Introduced on the S6100–ON, S6000, S6000–ON, S5000, S4810, S4820T, S3048–ON, S4048–ON, MXL, FN IOM, C9010, S3100, and Z9100-ON.

Related Commands

- show running-config — views the current configuration.
- privilege level (CONFIGURATION mode) — controls access to the command modes within the switch.

enable restricted

Allows Dell Networking technical support to access restricted commands.

C9000 Series

Syntax

`enable restricted [encryption-type] password`

To disallow access to restricted commands, use the `no enable restricted` command.

Parameters

encryption-type	(OPTIONAL) Enter the number `7` as the encryption type. Enter `7` followed a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults

Not configured.

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.0	Introduced on the E-Series.

Usage Information Only Dell Networking Technical Support staff use this command.

enable secret

Change the password for the `enable` command.

C9000 Series

Syntax `enable secret [level level] [encryption-type] password`

To delete a password, use the `no enable secret [encryption-type] password [level level]` command.

Parameters

level *level*	(OPTIONAL) Enter the keyword `level` then a number as the level of access. The range is from 1 to 15.
encryption-type	(OPTIONAL) Enter the number `5` or `0` as the encryption type. Enter a `5` then a text string as the hidden password. The text string must be a password that was already encrypted by a Dell Networking router. Use this parameter only with a password that you copied from the `show running-config` file of another Dell Networking router.
password	Enter a text string, up to 32 characters long, as the clear text password.

Defaults No password is configured. *level* = **15**.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

To control access to command modes, use this command to define a password for a level and use the `privilege level (CONFIGURATION mode)` command.

Passwords must meet the following criteria:

- Start with a letter, not a number.
- Passwords can have a regular expression as the password. To create a password with a regular expression in it, use CNTL + v prior to entering regular expression. For example, to create the password `abcd]e`, you type "`abcd CNTL v ]e`". When the password is created, you do not use the CNTL + v key combination and enter "`abcd]e`".

NOTE: The question mark (?) and the tilde (~) are not supported characters.

Related Commands

show running-config — views the current configuration.

privilege level (CONFIGURATION mode) — controls access to the command modes within the switch.

login authentication

To designate the terminal lines, apply an authentication method list.

C9000 Series

Syntax

`login authentication {`*`method-list-name`*` | default}`

To use the local user/password database for login authentication, use the `no login authentication` command.

Parameters

method-list-name	Enter the keywords `method-list-name` to specify that method list, created in the `aaa authentication login` command, to be applied to the designated terminal line.
default	Enter the keyword `default` to specify that the default method list, created in the `aaa authentication login` command, is applied to the terminal line.

Defaults

No authentication is performed on the console lines. Local authentication is performed on the virtual terminal and auxiliary lines.

Command Modes

LINE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information If you configure the `aaa authentication login default` command, the `login authentication default` command automatically is applied to all terminal lines.

Related Commands aaa authentication login — selects the login authentication methods.

password

Specify a password for users on terminal lines.

C9000 Series

Syntax `password [encryption-type] password`

To delete a password, use the `no password password` command.

Parameters

encryption-type	(OPTIONAL) Enter either zero (`0`) or `7` as the encryption type for the password entered. The options are • `0` is the default and means the password is not encrypted and stored as clear text. • `7` means that the password is encrypted and hidden.
password	Enter a text string up to 32 characters long. The first character of the password must be a letter. You cannot use spaces in the password.

Defaults No password is configured.

Command Modes LINE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.0	Introduced on the E-Series.

Usage Information The software prompts users for these passwords when the method for authentication or authorization used is "line".

Related Commands

enable password — sets the password for the `enable` command.

login authentication — configures an authentication method to log in to the switch.

service password-encryption — encrypts all passwords configured in the system.

radius-server key — configures a key for all RADIUS communications between the switch and the RADIUS host server.

tacacs-server key — configures a key for communication between a TACACS+ server and client.

username — establishes an authentication system based on user names.

password-attributes

Configure the password attributes (strong password).

C9000 Series

Syntax

`password-attributes [min-length` *`number`*`] [max-retry` *`number`*`] [lockout-period` *`minutes`*`][character-restriction [upper` *`number`*`] [lower` *`number`*`] [numeric` *`number`*`] [special-char` *`number`*`]]`

To return to the default, use the `no password-attributes [min-length` *`number`*`] [max-retry` *`number`*`] [lockout-period` *`minutes`*`] [character-restriction [upper` *`number`*`] [lower` *`number`*`] [numeric` *`number`*`] [special-char` *`number`*`]]` command.

Parameters

min-length *number*	(OPTIONAL) Enter the keywords `min-length` then the number of characters. The range is from 0 to 32 characters.
max-retry *number*	(OPTIONAL) Enter the keywords `max-retry` then the number of maximum password retries. The range is from 0 to 16.
lockout-period *minutes*	(OPTIONAL) Enter the keyword `lockout-period` then the number of minutes. The range is from `1` to `1440` minutes. The default is `0` minutes and the lockout-period is not enabled. This parameter enhances the security of the switch by locking out sessions on the Telnet or SSH sessions for which there has been a consecutive failed login attempts. The console is not locked out.
character-restriction	(OPTIONAL) Enter the keywords `character-restriction` to indicate a character restriction for the password.
upper *number*	(OPTIONAL) Enter the keyword `upper` then the upper number. The range is from 0 to 31.
lower *number*	(OPTIONAL) Enter the keyword `lower` then the lower number. The range is from 0 to 31.

numeric *number*	(OPTIONAL) Enter the keyword `numeric` then the numeric number. The range is from 0 to 31.
special-char *number*	(OPTIONAL) Enter the keywords `special-char` then the number of special characters permitted. The range is from 0 to 31.

Defaults 0 minutes for the lock out period. The lockout-period is not enabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced the `lockout-period` option on the Z9500.
9.5(0.0)	Introduced the `lockout-period` option on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Introduced on the E-Series.

Example In the following example, after 5 un-successful login attempts, the session (SSH/TELNET) goes into a locked state for 5 minutes. If all the 10 sessions are locked out with 5 un-successful attempts in each session, no users can login during the lockout-period.

```
Dell(conf)#password-attributes max-retry 5 lockout-period 5
```

Related Commands password — specifies a password for users on terminal lines.

service obscure-passwords

Enable the obscuring of passwords and keys.

C9000 Series

Syntax `service obscure-passwords`

Enable the obscuring of passwords and keys, including RADIUS, TACACS+ keys, router authentication strings, VRRP authentication, use the `service obscure-passwords` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6.0.0	Introduced on the S4810, S4820T, S5000, S6000, Z9000, Z9500, MXL

Usage Information By default, the `service password-encryption` command stores encrypted passwords. For greater security, you can also use the `service obscure-passwords` command to prevent a user from reading the passwords and keys, including RADIUS, TACACS+ keys, router authentication strings, VRRP authentication by obscuring this information. Passwords and keys are stored encrypted in the configuration file and by default are displayed in the encrypted form when the configuration is displayed. Enabling the `service obscure-passwords` command displays asterisks instead of the encrypted passwords and keys. This command prevents a user from reading these passwords and keys by obscuring this information with asterisks.

Password obscuring masks the password and keys for display only but does not change the contents of the file. The string of asterisks is the same length as the encrypted string for that line of configuration. To verify that you have successfully obscured passwords and keys, use the `show running-config` command or `show startup-config` command.

If you are using role-based access control (RBAC), only the system administrator and security administrator roles can enable the `service obscure-password` command.

Related Commands

- show running-config — Display the current configuration and display changes from the default values.
- service password-encryption— Encrypts all passwords configured in the system.

service password-encryption

Encrypt all passwords configured in the system.

C9000 Series

Syntax `service password-encryption`

To store new passwords as clear text, use the `no service password-encryption` command.

Defaults Enabled.

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

CAUTION: Encrypting passwords with this command does not provide a high level of security. When the passwords are encrypted, you cannot return them to plain text unless you re-configure them. To remove an encrypted password, use the `no password password` command.

To keep unauthorized people from viewing passwords in the switch configuration file, use the `service password-encryption` command. This command encrypts the clear-text passwords created for user name passwords, authentication key passwords, the privileged command password, and console and virtual terminal line access passwords.

To view passwords, use the `show running-config` command.

secure-cli enable

Enable the secured CLI mode.

Syntax `secure-cli enable`

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced this command.

Usage Information

The secured CLI mode prevents the users from enhancing the permissions or promoting the privilege levels. After entering the command, save the running-configuration.

Once you save the running-configuration, the secured CLI mode is enabled. If you do not want to enter the secured mode, do not save the running-configuration.

Once saved, to disable the secured CLI mode, you need to manually edit the startup-configuration file and reboot the system.

show privilege

View your access level.

C9000 Series

Syntax

```
show privilege
```

From a **PE console**, use `show privilege` to view the current privilege level.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show privilege
Current privilege level is 15
Dell#
```

Example (PE Console)

```
Dell#show privilege
Current privilege level is 15.
```

Related Commands

privilege level (CONFIGURATION mode) — assigns access control to different command modes.

show users

Allows you to view information on all users logged into the switch, including privilege level and or user role.

C9000 Series

Syntax `show users [all]`

Parameters

all	(OPTIONAL) Enter the keyword `all` to view all terminal lines in the switch.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for roles on the Z9500.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The following describes the `show users`command shown in the following example.

Field	Description
(untitled)	Indicates with an asterisk (*) which terminal line you are using.
Line	Displays the terminal lines currently in use.
User	Displays the user name of all users logged in.
Host(s)	Displays the terminal line status.
Location	Displays the IP address of the user.

Example

```
Dell#show users
Authorization Mode:  role or privilege

 Line         User     Role       Privilege Host(s) Location
 0 console 0  admin    sysadmin     15      idle
```

```
*3 vty 1       sec1      secadmin     14       idle     172.31.1.4
 4 vty 2       ml1       netadmin     12       idle     172.31.1.5
```

Related Commands username — use to enter the user name.

timeout login response

Specify how long the software waits for the login input (for example, the user name and password) before timing out.

C9000 Series

Syntax `timeout login response seconds`

To return to the default values, use the `no timeout login response` command.

Parameters

seconds Enter a number of seconds the software waits before logging you out. The range is:

- VTY: the range is from 1 to 30 seconds, the default is **30 seconds**.
- Console: the range is from 1 to 300 seconds, the default is **0 seconds** (no timeout).
- AUX: the range is from 1 to 300 seconds, the default is **0 seconds** (no timeout).

Defaults See the defaults settings shown in *Parameters*.

Command Modes LINE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The software measures the period of inactivity defined in this command as the period between consecutive keystrokes. For example, if your password is “password” you can enter “p” and wait 29 seconds to enter the next letter.

username

Establish an authentication system based on user names.

Syntax

`username name [access-class access-list-name] [nopassword | {password | secret | sha256-password} [encryption-type] password [dynamic-salt]] [privilege level] [role role-name]`

If you do not want a specific user to enter a password, use the `nopassword` option.

To delete authentication for a user, use the `no username name` command.

Parameters

name	Enter a text string for the name of the user up to 63 characters.
access-class *access-list-name*	Enter the keywords `access-class` then the name of a configured access control list (either an IP access control list or MAC access control list).
nopassword	Enter the keyword `nopassword` to specify that the user should not enter a password.
password	Enter the keyword `password` then the `encryption-type` or the password.
encryption-type	Enter an encryption type for the `password` that you enter. • `0` directs the system to store the password as clear text. It is the default encryption type when using the `password` option. • `8` to indicate that a password encrypted using a sha256 hashing algorithm follows. This encryption type is available with the `sha256-password` option only, and is the default encryption type for this option. • `7` to indicate that a password encrypted using a DES hashing algorithm follows. This encryption type is available with the `password` option only. • `5` to indicate that a password encrypted using an MD5 hashing algorithm follows. This encryption type is available with the `secret` option only, and is the default encryption type for this option.
password	Enter a string up to 32 characters long.
dynamic-salt	Enter the keyword `dynamic-salt` to have an additional random input in the password encryption process.
privilege *level*	Enter the keyword `privilege` then a number from zero (0) to 15.
role *role-name*	Enter the keyword `role` followed by the role name to associate with that user ID.
secret	Enter the keyword `secret` then the encryption type.
sha256-password	Enter the keyword `sha256-password` then the `encryption-type` or the password.

Defaults

The default encryption type for `password` option is **0**. The default encryption type for `secret` option is **5**. The default encryption type for `sha256-password` option is **8**. The default value of `privilege level` is **1**.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13.0.0	Enhanced to display a warning message when a weak password is used. Introduced the `dynamic-salt` option on the MXL, S5000, S4048-ON, S6000, S6000-ON, S3048-ON, S3100 Series, C9010, S4048T-ON, Z9500, Z9100-ON, S6100-ON, S6010-ON.
9.12(1.0)	Introduced on the S5048F–ON.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Added support for the `sha256-password` option for S3100, S3048–ON, S4048–ON, S4810, S4820T, S5000, S6000, S6000–ON, Z9100–ON, MXL, and Z9500.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100-ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000–ON.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added support for the `secret` option and the MD5 password encryption. Extended the name from 25 to 63 characters.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

Usage Information

To view the defined user names, use the `show running-config user` command. You can use the `dynamic-salt` option only under the `secret` and the `password` options.

When you configure the password, the system alerts if your password does not match the following criteria. The system accepts your password even if these conditions are not met. Dell EMC Networking recommends selecting a strong password for enhanced security.

- A minimum of eight characters in length
- A minimum of one lower case letter (a to z)
- A minimum of one upper case letter (A to Z)
- A minimum of one numeric character (0 to 9)
- A minimum of one special character including a space (" !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~")

Related Commands

- password — specifies a password for users on terminal lines.
- show running-config — views the current configuration.

RADIUS Commands

The following RADIUS commands are supported by Dell Networking OS.

aaa radius auth-method

Configure the authentication method to use with RADIUS for user access.

Syntax

```
aaa radius auth-method {pap | mschapv2}
```

To undo the RADIUS authentication method configuration, use the `no aaa radius auth-method` command.

Parameters

pap	Enter the keyword `pap` to use the Password Authentication Protocol (PAP) for RADIUS authentication. This protocol uses the username and password attributes in the access-request message sent to the RADIUS server.
mschapv2	Enter the keyword `mschapv2` to use the Microsoft Challenge-Handshake Authentication Protocol (MS-CHAPv2) for RADIUS authentication. This protocol is considered to be more secure than PAP and uses mutual authentication based on a random challenge and challenge response.

Defaults

PAP

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(2.0P2)	Introduced the command on all Dell Networking OS platforms.

Usage Information

If an authentication method is not configured using this command, then PAP is used for authentication with the RADIUS server.

You can configure the RADIUS authentication method to access the switch using the following applications: Console, Telnet, SSH, REST, and OMI.

client

Configures trusted DAC clients.

Syntax

```
client {ipv4-addr | ipv6-addr | hostname} [vrf vrf-name] [key [encryption-type] key]
```

To undo the DAC client configuration, enter the `no client host` command.

Defaults

If VRF is not configured, default VRF is considered.

Parameters

ipv4–addr	Enter the keyword `ipv4-addr` to specify the IPv4 address of the DAC.

ipv6–addr	Enter the keyword `ipv6-addr` to specify the IPv6 address of the DAC.
hostname	Enter the keyword `hostname` to enter the name of the host.
vrf *vrf-name*	Enter the keyword `vrf` followed by the name of the VRF to associate a VRF with the client.
key	(Optional) Enter the keyword `key` to specify an encryption key.
encryption-type	(Optional) Enter either 0 or 7 as the encryption type for the specified key. The options are: • 0 – implies that the key is not encrypted and is stored as clear text. • 7 – implies that the key is encrypted and hidden.
key	Enter a string that is the key to be exchanged between the switch and the dynamic authorization client. The key can be up to 42 characters long.

Command Modes

- CONF-DYNAMIC-AUTH

Usage Information

- It is possible to configure more than one dynamic authorization clients Duplicate (ipv4-addr or ipv6-addr or host-name) configurations are not allowed.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FM-IOM, and MXL.

client-key

Configures global shared key for the trusted DAC clients.

Syntax

`client–key [encryption-type] key`

To remove the shared key configuration, enter the no `client-key` command.

Defaults

None.

Parameters

encryption-type:	(OPTIONAL) Enter either 0 or 7 as the encryption type for the key entered. The options are: • 0 — is the default and means the key is not encrypted and stored as clear text. • 7 — means that the key is encrypted and hidden.
key	Enter a string that is the key to be exchanged between the switch and RADIUS servers. It can be up to 42 characters long.

Command Modes

- CONF-DYNAMIC-AUTH

Usage Information

- Configure global shared key applicable for DA clients. If client configuration has shared key configured, that will take precedence.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

coa-bounce-port

Configure NAS to ignore the port bounce RADIUS messages from DAC.

Syntax

```
coa-bounce-port
```

To remove the port bounce configuration, enter the `no coa-bounce-port` command.

Defaults

Enabled.

Command Modes

- CONF-DYNAMIC-AUTH

Usage Information

- Configure `no coa-bounce-port` to drop radius CoA port-bounce requests from the DAC.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

coa-disable-port

Configure NAS to reject disable-port requests from DAC.

Syntax

```
coa-disable-port
```

To undo this configuration, enter the `no coa-disable-port` command.

Defaults

Enabled.

Command Modes

- CONF-DYNAMIC-AUTH

Usage Information

- Configure `no coa-disable-port` DAS to drop radius CoA disable-port requests from DAC.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

coa-reauthenticate

Configure NAS to re-authenticate dot1x user session requests from DAC.

Syntax

`coa-reauthenticate`

To ignore re-authentication requests, enter the `no coa-reauthenticate` command.

Defaults

Enabled.

Command Modes

- CONF-DYNAMIC-AUTH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

debug radius

View RADIUS transactions to assist with troubleshooting.

C9000 Series

Syntax

`debug radius`

To disable debugging of RADIUS, use the `no debug radius` command.

Defaults

Disabled.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

da-rsp-timeout

Configure timeout value for the back end task to respond to DAC requests.

Syntax

`da-rsp-timeout` *minutes*

To undo the configuration, enter the `no da-rsp-timeout` command.

Defaults

10 Minutes.

Parameters

minutes	Enter the time out value.

Command Modes

- CONF-DYNAMIC-AUTH

Usage Information

- Time for DAS to wait before the back end response is received.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

disconnect-user

Configure NAS to ignore DM requests corresponding to AAA users-sessions coming from the DAC.

Syntax

```
disconnect-user
```

To undo this configuration, enter the `no disconnect-user` command.

Defaults

Enabled.

Command Modes

- CONF-DYNAMIC-AUTH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

dynamic-auth-enable

Configure NAS to receive and process dynamic authorization messages.

Syntax

```
dynamic-auth-enable
```

To stop NAS from receiving and processing dynamic authorization messages, use the `no dynamic-auth-enable` command.

Defaults

Disabled.

Command Modes

- CONF-DYNAMIC-AUTH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

Usage Information

If this configuration is not enabled, then dynamic authorization messages are not handled by the NAS.

ip radius source-interface

Specify an interface's IP address as the source IP address for RADIUS connections.

C9000 Series

Syntax

`ip radius source-interface` *interface*

To delete a source interface, use the `no ip radius source-interface` command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16838.
- For the Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

port

Configures NAS port number to accept CoA or DM requests.

Syntax

`port port-number`

To remove the NAS port configuration, enter the `no port` command.

Defaults

3799

Parameters

port-number	Enter the NAS port number to accept CoA and DM requests. The range is from 1 to 65535.

Command Modes

- CONF-DYNAMIC-AUTH

Usage Information

- Optionally specify dynamic authorization port number. Default port is 3799.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

radius dynamic-auth

Enters a new sub-mode, RADIUS-DYNAMIC-AUTH, which enables you to modify dynamic authorization settings.

Syntax

`radius dynamic-auth`

To remove the dynamic authorization method for RADIUS users, enter the `no radius dynamic-auth` command.

Defaults

Disabled.

Command Modes

- CONFIGURATION

Usage Information

- All dynamic authorization commands are configured by entering this mode.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

radius-server deadtime

Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

C9000 Series

Syntax

`radius-server deadtime` *seconds*

To disable this function or return to the default value, use the `no radius-server deadtime` command.

Parameters

seconds	Enter a number of seconds during which non-responsive RADIUS servers are skipped. The range is from 0 to 2147483647 seconds. The default is **0 seconds**.

Defaults

0 seconds

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

radius-server host

Configure a RADIUS server host.

C9000 Series

Syntax

```
radius-server host {hostname | ipv4-address | ipv6-address} [auth-port port-number] [retransmit retries] [timeout seconds] [key [encryption-type] key]
```

Parameters

hostname	Enter the name of the RADIUS server host.
ipv4-address | *ipv6-address*	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) of the RADIUS server host.
auth-port *port-number*	(OPTIONAL) Enter the keywords `auth-port` then a number as the port number. The range is from zero (0) to 65535. The default port-number is **1812**.
retransmit *retries*	(OPTIONAL) Enter the keyword `retransmit` then a number as the number of attempts. This parameter overwrites the `radius-server retransmit` command. The range is from zero (0) to 100. The default is **3 attempts**.
timeout *seconds*	(OPTIONAL) Enter the keyword `timeout` then the seconds the time interval the switch waits for a reply from the RADIUS server. This parameter overwrites the `radius-server timeout` command. The range is from 0 to 1000. The default is **5 seconds**.
key [*encryption-type*] *key*	(OPTIONAL) Enter the keyword `key` then an optional encryption-type and a string up to 42 characters long as the authentication key. The RADIUS host server uses this authentication key and the RADIUS daemon operating on this switch. For the encryption-type, enter either zero (`0`) or `7` as the encryption type for the key entered. The options are: • `0` is the default and means the password is not encrypted and stored as clear text. • `7` means that the password is encrypted and hidden. Configure this parameter last because leading spaces are ignored.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.4.1.0	Added support for IPv6.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Authentication key length increased to 42 characters.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

To configure any number of RADIUS server hosts for each server host that is configured, use this command. The system searches for the RADIUS hosts in the order they are configured in the software.

The global default values for the `timeout`, `retransmit`, and `key` optional parameters are applied, unless those values are specified in the `radius-server host` or other commands. To return to the global default values, if you configure the `timeout`, `retransmit`, or `key` values, include those keywords when using the `no radius-server host` command syntax.

Related Commands

login authentication — sets the database to be checked when a user logs in.

radius-server key — sets an authentication key for RADIUS communications.

radius-server retransmit — sets the number of times the RADIUS server attempts to send information.

radius-server timeout — sets the time interval before the RADIUS server times out.

radius-server key

Configure a key for all RADIUS communications between the switch and the RADIUS host server.

C9000 Series

Syntax

`radius-server key [`*`encryption-type`*`] `*`key`*

To delete a password, use the `no radius-server key` command.

Parameters

encryption-type	(OPTIONAL) Enter either zero (`0`) or `7` as the encryption type for the key entered. The options are: • `0` is the default and means the key is not encrypted and stored as clear text. • `7` means that the key is encrypted and hidden.
key	Enter a string that is the key to be exchanged between the switch and RADIUS servers. It can be up to 42 characters long.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Authentication key length increased to 42 characters.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Usage Information

The key configured on the switch must match the key configured on the RADIUS server daemon.

If you configure the `key` parameter in the `radius-server host` command, the key configured with the `radius-server key` command is the default key for all RADIUS communications.

Related Commands

radius-server host — configures a RADIUS host.

radius-server retransmit

Configure the number of times the switch attempts to connect with the configured RADIUS host server before declaring the RADIUS host server unreachable.

C9000 Series

Syntax

`radius-server retransmit` *`retries`*

To configure zero retransmit attempts, use the `no radius-server retransmit` command.

To return to the default setting, use the `radius-server retransmit 3` command.

Parameters

retries	Enter a number of attempts that the system tries to locate a RADIUS server. The range is from zero (0) to 100. The default is **3 retries**.

Defaults

3 retries

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

Related Commands radius-server host — configures a RADIUS host.

radius-server timeout

To reply to a request, configure the amount of time the RADIUS client (the switch) waits for a RADIUS host server .

C9000 Series

Syntax `radius-server timeout` *seconds*

To return to the default value, use the `no radius-server timeout` command.

Parameters

seconds	Enter the number of seconds between an unsuccessful attempt and when the system times out. The range is from zero (0) to 1000 seconds. The default is **5 seconds**.

Defaults **5 seconds**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.2.1.0	Introduced on the E-Series.

Related Commands radius-server host — configures a RADIUS host.

rate-limit

Configure NAS to allow or reject RADIUS dynamic authorization (DA) packets based on the configurable rate limit value.

Syntax

```
rate-limit packets per minute
```

To undo the configuration, enter the `no rate-limit` command.

Defaults 30 packets per minute.

Parameters

packet per minute	Enter the number of packets that you want processed per minute. The range is between 10 to 60 packets per minute.

Command Modes

- CONF-DYNAMIC-AUTH

Usage Information

- Packets are dropped after number of packets reaches the configured rate-limit.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

replay-protection-window

Configure replay protection window period to drop the duplicate packets.

Syntax

```
replay-protection-window minutes
```

To undo the configuration, enter the `no replay-protection-window` command.

Defaults 5 Minutes.

Parameters

minutes	Enter the number of minutes to drop the packets. The range is from 1 to 10 minutes.

Command Modes

- CONF-DYNAMIC-AUTH

Usage Information

- Duplicate packets are dropped within replay-protection-window period if packet has same source IP address, source UDP port and identifier.

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

terminate-session

Configure NAS to reject dot1x terminate-session requests from DAC.

Syntax

```
terminate-session
```

To drop the DM terminate-session requests from DAC, enter the `no terminate-session` command.

Defaults

Enabled.

Command Modes

- CONF-DYNAMIC-AUTH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

The following is a list of the Dell EMC Networking OS version history for this command.

Version	Description
9.13(0.0)	Introduced on the C9010, S3100, S3048–ON, S4048T-ON, S4048–ON, S5000, S6010–ON, S6000–ON, S6100–ON, S6000, Z9100–ON, Z9500, FN-IOM, and MXL.

TACACS+ Commands

The Dell Networking OS supports TACACS+ as an alternate method for login authentication.

debug tacacs+

To assist with troubleshooting, view TACACS+ transactions.

C9000 Series

Syntax

```
debug tacacs+
```

To disable debugging of TACACS+, use the `no debug tacacs+` command.

Defaults Disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.0	Introduced on the E-Series.

ip tacacs source-interface

Specify an interface's IP address as the source IP address for TACACS+ connections.

C9000 Series

Syntax `ip tacacs source-interface` *interface*

To delete a source interface, use the `no ip tacacs source-interface` command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16838.
- For the Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

tacacs-server host

Specify a TACACS+ host.

C9000 Series

Syntax

```
tacacs-server host {hostname | ipv4-address | ipv6-address} [port number]
[timeout seconds] [key key]
```

Parameters

hostname	Enter the name of the TACACS+ server host.
ipv4-address | *ipv6-address*	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) of the TACACS+ server host.
port *number*	(OPTIONAL) Enter the keyword `port` then a number as the port to be used by the TACACS+ server. The range is from zero (0) to 65535. The default is **49**.
timeout *seconds*	(OPTIONAL) Enter the keyword `timeout` then the number of seconds the switch waits for a reply from the TACACS+ server. The range is from 0 to 1000. The default is **10 seconds**.
key *key*	(OPTIONAL) Enter the keyword `key` then a string up to 42 characters long as the authentication key. This authentication key must match the key specified in the `tacacs-server key` for the TACACS+ daemon.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Added support for IPv6.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Authentication key length increased to 42 characters.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

To list multiple TACACS+ servers to be used by the `aaa authentication login` command, configure this command multiple times.

If you are not configuring the switch as a TACACS+ server, you do not need to configure the `port`, `timeout` and `key` optional parameters. If you do not configure a key, the key assigned in the `tacacs-server key` command is used.

Related Commands

aaa authentication login — specifies the login authentication method.

tacacs-server key — configures a TACACS+ key for the TACACS server.

tacacs-server key

Configure a key for communication between a TACACS+ server and a client.

C9000 Series

Syntax

`tacacs-server key [`*`encryption-type`*`] key`

To delete a key, use the `no tacacs-server key` *`key`* command.

Parameters

encryption-type	(OPTIONAL) Enter either zero (`0`) or `7` as the encryption type for the key entered. The options are: • `0` is the default and means the key is not encrypted and stored as clear text. • `7` means that the key is encrypted and hidden.
key	Enter a text string, up to 42 characters long, as the clear text password. Leading spaces are ignored.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Authentication key length increased to 42 characters.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information The key configured with this command must match the key configured on the TACACS+ daemon.

Port Authentication (802.1X) Commands

An authentication server must authenticate a client connected to an 802.1X switch port. Until the authentication, only Extensible Authentication Protocol over LAN (EAPOL) traffic is allowed through the port to which a client is connected. After authentication is successful, normal traffic passes through the port.

The Dell Networking OS supports RADIUS and Active Directory environments using 802.1X Port Authentication.

Important Points to Remember

The system limits network access for certain users by using VLAN assignments. 802.1X with VLAN assignment has these characteristics when configured on the switch and the RADIUS server.

- 802.1X is not supported on the LAG or the channel members of a LAG.
- If no VLAN is supplied by the RADIUS server or if 802.1X authorization is disabled, the port is configured in its access VLAN after successful authentication.
- If 802.1X authorization is enabled but the VLAN information from the RADIUS server is not valid, the port returns to the Unauthorized state and remains in the configured access VLAN. This prevents ports from appearing unexpectedly in an inappropriate VLAN due to a configuration error. Configuration errors create an entry in Syslog.
- If 802.1X authorization is enabled and all information from the RADIUS server is valid, the port is placed in the specified VLAN after authentication.
- If port security is enabled on an 802.1X port with VLAN assignment, the port is placed in the RADIUS server assigned VLAN.
- If 802.1X is disabled on the port, it is returned to the configured access VLAN.
- When the port is in the Force Authorized, Force Unauthorized, or Shutdown state, it is placed in the configured access VLAN.
- If an 802.1X port is authenticated and put in the RADIUS server assigned VLAN, any change to the port access VLAN configuration does not take effect.

- The 802.1X with VLAN assignment feature is not supported on trunk ports, dynamic ports, or with dynamic-access port assignment through a VLAN membership.

dot1x authentication (Configuration)

Enable dot1x globally. Enable dot1x both globally and at the interface level.

C9000 Series

Syntax

```
dot1x authentication
```

To disable dot1x globally, use the `no dot1x authentication` command.

Defaults

Disabled

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

Related Commands

dot1x authentication (Interface)

dot1x authentication (Interface)

Enable dot1x on an interface; dot1x must be enabled both globally and at the interface level.

C9000 Series

Syntax

```
dot1x authentication
```

To disable dot1x on an interface, use the `no dot1x authentication` command.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands dot1x authentication (Configuration) — enables dot1x globally.

dot1x auth-fail-vlan

Configure an authentication failure VLAN for users and devices that fail 802.1X authentication.

C9000 Series

Syntax `dot1x auth-fail-vlan` *`vlan-id`* `[max-attempts` *`number`*`]`

To delete the authentication failure VLAN, use the `no dot1x auth-fail-vlan` *`vlan-id`* `[max-attempts` *`number`*`]` command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is from 1 to 4094.
max-attempts *number*	(OPTIONAL) Enter the keywords `max-attempts` then number of attempts desired before authentication fails. The range is from 1 to 5. The default is **3**.

Defaults **3 attempts**

Command Modes CONFIGURATION (conf-if-interface-slot/port)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series, S-Series, and E-Series.

Usage Information

If the host responds to 802.1X with an incorrect login/password, the login fails. The switch attempts to authenticate again until the maximum attempts configured is reached. If the authentication fails after all allowed attempts, the interface is moved to the authentication failed VLAN.

After the authentication VLAN is assigned, the port-state must be toggled to restart authentication. Authentication occurs at the next re-authentication interval (`dot1x reauthentication`).

Related Commands

dot1x port-control — enables port-control on an interface.

dot1x guest-vlan — configures a guest VLAN for non-dot1x devices.

show dot1x interface — displays the 802.1X information on an interface.

dot1x auth-server

Configure the authentication server to RADIUS.

C9000 Series

Syntax `dot1x auth-server radius`

Defaults none

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the C-Series and S-Series.

Version	Description
7.4.1.0	Introduced on the E-Series.

dot1x guest-vlan

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

C9000 Series

Syntax

`dot1x guest-vlan` *vlan-id*

To disable the guest VLAN, use the `no dot1x guest-vlan` *vlan-id* command.

Parameters

vlan-id	Enter the VLAN Identifier. The range is from 1 to 4094.

Defaults

Not configured.

Command Modes

CONFIGURATION (conf-if-interface-slot/port)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series, S-Series, and E-Series.

Usage Information

802.1X authentication is enabled when an interface is connected to the switch. If the host fails to respond within a designated amount of time, the authenticator places the port in the guest VLAN.

If a device does not respond within 30 seconds, it is assumed that the device is not 802.1X capable. Therefore, a guest VLAN is allocated to the interface and authentication for the device occurs at the next re-authentication interval (`dot1x reauthentication`).

If the host fails authentication for the designated number of times, the authenticator places the port in authentication failed VLAN (`dot1x auth-fail-vlan`).

NOTE: The layer 3 portion of guest VLAN and authentication fail VLANs can be created regardless if the VLAN is assigned to an interface or not. After an interface is assigned a guest VLAN (which has an IP address), routing through the guest VLAN is the same as any other traffic. However, the interface may join/leave a VLAN dynamically.

Related Commands

dot1x auth-fail-vlan — configures a VLAN for authentication failures.

dot1x reauthentication — enables periodic re-authentication.

show dot1x interface — displays the 802.1X information on an interface.

dot1x mac-auth-bypass

Enable MAC authentication bypass. If 802.1X times out because the host did not respond to the Identity Request frame, the system attempts to authenticate the host based on its MAC address.

C9000 Series

Syntax

```
[no] dot1x mac-auth-bypass
```

Defaults

Disabled

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.4	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Introduced on the C-Series and S-Series.

Usage Information

To disable MAC authentication bypass on a port, enter the `no dot1x mac-auth-bypass` command.

dot1x max-eap-req

Configure the maximum number of times an extensive authentication protocol (EAP) request is transmitted before the session times out.

C9000 Series

Syntax

```
dot1x max-eap-req number
```

To return to the default, use the `no dot1x max-eap-req` command.

Parameters

number	Enter the number of times an EAP request is transmitted before a session time-out. The range is from 1 to 10. The default is **2**.

Defaults **2**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands interface range — configures a range of interfaces.

dot1x port-control

Enable port control on an interface.

C9000 Series

Syntax `dot1x port-control {force-authorized | auto | force-unauthorized}`

Parameters

force-authorized	Enter the keywords `force-authorized` to forcibly authorize a port.
auto	Enter the keyword `auto` to authorize a port based on the 802.1X operation result.
force-unauthorized	Enter the keywords `force-unauthorized` to forcibly de-authorize a port.

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information The authenticator performs authentication only when `port-control` is set to `auto`.

dot1x quiet-period

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

C9000 Series

Syntax `dot1x quiet-period` *seconds*

To disable quiet time, use the `no dot1x quiet-time` command.

Parameters

seconds	Enter the number of seconds. The range is from 1 to 65535. The default is **30**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x reauthentication

Enable periodic re-authentication of the client.

C9000 Series

Syntax

`dot1x reauthentication [interval seconds]`

To disable periodic re-authentication, use `the no dot1x reauthentication` command.

Parameters

interval *seconds*	(Optional) Enter the keyword `interval` then the interval time, in seconds, after which re-authentication is initiated. The range is from 1 to 31536000 (1 year). The default is **3600 (1 hour)**.

Defaults

3600 seconds (1 hour)

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands

interface range — configures a range of interfaces.

dot1x reauth-max

Configure the maximum number of times a port can re-authenticate before the port becomes unauthorized.

C9000 Series

Syntax

`dot1x reauth-max number`

To return to the default, use the `no dot1x reauth-max` command.

Parameters

number — Enter the permitted number of re-authentications. The range is from 1 to 10. The default is **2**.

Defaults **2**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x server-timeout

Configure the amount of time after which exchanges with the server time-out.

C9000 Series

Syntax `dot1x server-timeout` *seconds*

To return to the default, use the `no dot1x server-timeout` command.

Parameters

seconds — Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time-out.

C9000 Series

Syntax

`dot1x supplicant-timeout` *seconds*

To return to the default, use the`no dot1x supplicant-timeout` command.

Parameters

seconds	Enter a time-out value in seconds. The range is from 1 to 300, where 300 is implementation dependant. The default is **30**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x tx-period

Configure the intervals at which EAPOL PDUs are transmitted by the Authenticator PAE.

C9000 Series

Syntax

```
dot1x tx-period seconds
```

To return to the default, use the `no dot1x tx-period` command.

Parameters

seconds	Enter the interval time, in seconds, that EAPOL PDUs are transmitted. The range is from 1 to 31536000 (1 year). The default is **30**.

Defaults **30 seconds**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

show dot1x interface

Display the 802.1X information on an interface.

C9000 Series

Syntax

```
show dot1x interface interface
```

Parameters

interface	Enter one of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.

- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series, S-Series, and E-Series.

Example

```
Dell#show dot1x int  Te 2/32
802.1x information on   Te 2/32:
-----------------------------
Dot1x Status:           Enable
Port Control:           AUTO
Port Auth Status:       UNAUTHORIZED
Re-Authentication:      Disable
Untagged VLAN id:       None
Guest VLAN:             Enable
Guest VLAN id:          10
Auth-Fail VLAN:         Enable
Auth-Fail VLAN id:      11
Auth-Fail Max-Attempts: 3
Tx Period:              30 seconds
Quiet Period:           60 seconds
ReAuth Max:             2
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       3600 seconds
Max-EAP-Req:            2
Auth Type:              SINGLE_HOST
Auth PAE State:         Initialize
Backend State:          Initialize
Dell#
```

SSH Server and SCP Commands

The Dell Networking OS supports secure shell (SSH) protocol versions 1.5 and 2.0. SSH is a protocol for secure remote login over an insecure network. SSH sessions are encrypted and use authentication.

crypto cert generate

Generates a default key and a self-signed certificate. This command replaces the existing certificate with a new certificate.

C9000 Series

Syntax

```
crypto cert generate {cert-file file-name key-file file-name} [cname common-name] [country country-name] [email email-id] [length key-length] [locality locality-name] [organization organization-name] [orgunit organization-unit-name] [state state-name] [validity days]
```

Parameters

cert-file *file-name*	Enter the keyword `cert-file` then the filename of the certificate to be generated.
key-file *file-name*	Enter the keyword `key-file` then the key filename to be generated.
cname *common-name*	(OPTIONAL) Enter the keyword `cname` then the common name to be included in the certificate. The default is Dell Networking.
country *country-name*	(OPTIONAL) Enter the keyword `country` then the name of the country to be included in the certificate. The maximum number of characters allowed for the country-name is two. The default is US.
email *email-id*	(OPTIONAL) Enter the keyword `email` then the email-id to be included in the certificate.
length *key-length*	(OPTIONAL) Enter the keyword `length` then the key length in bits. The key length range is from 1024 to 4096 bits. The default is 2048 bits.
locality *locality-name*	(OPTIONAL) Enter the keyword `locality` then the name of the locality to be included in the certificate. The default is San Jose.
organization *organization-name*	(OPTIONAL) Enter the keyword `organization` then the name of the organization to be included in the certificate. The default is Dell.
orgunit *organization-unit-name*	(OPTIONAL) Enter the keyword `orgunit` then the organization unit name to be included in the certificate. The default is Dell Networking.
state *state-name*	(OPTIONAL) Enter the keyword `state` then the name of the state to be included in the certificate. The default is California.
validity *days*	(OPTIONAL) Enter the keyword `validity` then the number of days the certificate is valid. The validity range is from 1 to 10000 days. The default value is 3650 days (10 years).

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Introduced on the S -Series and Z-Series switches.

Usage Information The maximum number of characters allowed for the parameters, except the county-name, is **64**.

crypto key generate

Generate keys for the SSH server.

C9000 Series

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
crypto key generate {rsa | rsa1}
```

Parameters

rsa Enter the keyword `rsa` then the key size to generate a SSHv2 RSA host keys. The range is from 1024 to 2048 if you did not enable FIPS mode; if you enabled FIPS mode, you can only generate a 2048-bit key. The default is **1024**.

NOTE: You must have a license to access the FIPS mode. For more information, contact your Dell Networking representative.

rsa1 Enter the keyword `rsa1` then the key size to generate a SSHv1 RSA host keys. The range is from 1024 to 2048. The default is **1024**.

NOTE: This option is not available in FIPS mode.

Defaults Key size **1024**; if you enable FIPS mode, the key size is **2048**.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Added support for FIPS mode on the S4810.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The host keys are required for key-exchange by the SSH server. If the keys are not found when you enable the server (`ip ssh server enable`), the keys are automatically generated.

This command requires user interaction and generates a prompt prior to overwriting any existing host keys.

NOTE: Only a user with superuser permissions should generate host-keys.

Example

```
Dell#conf
Dell(conf)#crypto key generate rsa1
Enter key size <1024-2048>. Default<1024>: 1024

Host key already exists. Do you want to replace. [y/n] :y
Dell(conf)#
```

Related Commands

ip ssh server — enables the SSH server.

show crypto — displays the SSH host public keys.

crypto key zeroize rsa

Removes the generated RSA host keys and zeroize the key storage location.

C9000 Series

Syntax `crypto key zeroize rsa`

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Related Commands crypto key generate — Generate keys for SSH server

debug ip ssh

Enables collecting SSH debug information.

C9000 Series

Syntax `debug ip ssh {client | server}`

To disable debugging, use the `no debug ip ssh {client | server}` command.

Parameters

client	Enter the keyword `client` to enable collecting debug information on the client.
server	Enter the keyword `server` to enable collecting debug information on the server.

Defaults Disabled on both client and server.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information Debug information includes details for key-exchange, authentication, and established session for each connection.

ip scp topdir

Identify a location for files used in secure copy transfer.

C9000 Series

Syntax `ip scp topdir` *directory*

To return to the default setting, use the `no ip scp topdir` command.

Parameters

directory	Enter a directory name.

Defaults The internal flash (`flash:`) is the default directory.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information To configure the switch as an SCP server, use the `ip ssh server` command.

Related Commands ip ssh server — enables the SSH and SCP server on the switch.

ip ssh authentication-retries

Configure the maximum number of attempts that should be used to authenticate a user.

C9000 Series

Syntax `ip ssh authentication-retries 1-10`

Parameters

1-10	Enter the number of maximum retries to authenticate a user. The range is from 1 to 10. The default is **3**.

Defaults **3**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information This command specifies the maximum number of attempts to authenticate a user on an SSH connection with the remote host for password authentication. SSH disconnects when the number of password failures exceeds authentication-retries.

ip ssh challenge–response–authentication

Enable challenge response authentication for SSHv2.

Syntax `ip ssh challenge-response-authentication enable`

To disable the challenge response authentication, use the `no ip ssh challenge-response-authentication enable` command.

Parameters

enable Enter the keyword `enable` to enable the challenge response authentication for SSHv2.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the S4810, S4820T, S3048–ON, S3100 Series, S4048–ON, S5000, S6000, S6000–ON, Z9500, Z9100–ON, S6100–ON, S6010–ON, S4048T–ON, C9000, and MXL.

Usage Information If both the challenge response authentication and password authentication methods are configured, the challenge response authentication takes priority.

NOTE:

SSHv1 does not support challenge response authentication.

ip ssh cipher

Configure the list of ciphers supported on both SSH client and SCP.

Syntax `ip ssh cipher` *`cipher-list`*

Parameters

cipher *cipher-list* Enter the keyword `cipher` and then a space-delimited list of ciphers that the SSH client supports. The following ciphers are available.

- `aes256-ctr`
- `aes256-cbc`
- `aes192-ctr`
- `aes192-cbc`
- `aes128-ctr`
- `aes128-cbc`
- `3des-cbc`

Defaults The default list of ciphers is in the order as shown below:

- `aes256-ctr`
- `aes256-cbc`
- `aes192-ctr`
- `aes192-cbc`
- `aes128-ctr`
- `aes128-cbc`
- `3des-cbc`

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.0)	Introduced on the S6100–ON, S6000, S6000–ON, S5000, S4810, S4820T, S3048–ON, S4048–ON, MXL, C9010, S3100 series, and Z9100-ON.

Usage Information

- You can select one or more ciphers from the list.
- The default list of supported ciphers is same irrespective of whether FIPS mode is enabled or disabled.
- Client-supported cipher list gets preference over the server-supported cipher list in selecting the cipher for the SSH session.
- When the `cipher (-c)` option is used with the SSH CLI, it overrides the configured or default cipher list.
- When FIPS is enabled or disabled, the client ciphers get default configuration.

ip ssh connection-rate-limit

Configure the maximum number of incoming SSH connections per minute.

C9000 Series

Syntax `ip ssh connection-rate-limit 1-10`

Parameters

1-10	Enter the number of maximum numbers of incoming SSH connections allowed per minute. The range is from 1 to 10 per minute. The default is **10 per minute**.

Defaults **10 per minute**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ip ssh hostbased-authentication

Enable hostbased-authentication for the SSHv2 server.

C9000 Series

Syntax

```
ip ssh hostbased-authentication enable
```

To disable hostbased-authentication for SSHv2 server, use the `no ip ssh hostbased-authentication enable` command.

Parameters

enable	Enter the keyword `enable` to enable hostbased-authentication for SSHv2 server.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

If you enable this command, clients can log in without a password prompt. This command provides two levels of authentication:

- rhost-authentication is done with the file specified in the `ip ssh rhostfile` command.
- checking client host-keys is done with the file specified in the `ip ssh pub-key-file` command.

NOTE: Administrators must specify the two files (`rhosts` and `pub-key-file`) to configure host-based authentication.

Related Commands

ip ssh pub-key-file — public keys of trusted hosts from a file.

ip ssh rhostsfile — trusted hosts and users for rhost authentication.

ip ssh key-size

Configure the size of the server-generated RSA SSHv1 key.

C9000 Series

Syntax

```
ip ssh key-size 512-869
```

Parameters

512-869	Enter the key-size number for the server-generated RSA SSHv1 key. The range is from 512 to 869. The default is **768**.

Defaults

Key size **768**

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The server-generated key is used for SSHv1 key-exchange.

ip ssh mac

Configure the list of MAC algorithms supported on both SSH client and SCP.

Syntax `ip ssh mac mac-list`

Parameters

mac *mac-list*

Enter the keyword `mac` then a space-delimited list of message authentication code (MAC) algorithms supported by the SSH client. The following MAC algorithms are available.

When FIPS mode is enabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`

When FIPS mode is disabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-md5`
- `hmac-md5-96`

Defaults

The default list of MAC algorithm is in the order as shown below:

When FIPS mode is enabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`

When FIPS mode is disabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-md5`
- `hmac-md5-96`

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.0)	Introduced on the S6100–ON, S6000, S6000–ON, S5000, S4810, S4820T, S3048–ON, S4048–ON, MXL, C9010, S3100 series, and Z9100-ON.

Usage Information

- You can select one or more MAC algorithms from the list.
- Client-supported MAC list gets preference over the server-supported MAC list in selecting the MAC algorithm for the SSH session.
- When the `MAC (-m)` option is used with the SSH CLI, it overrides the configured or default MAC list.
- When FIPS is enabled or disabled, the client MACs get default configuration.

ip ssh password-authentication

Enable password authentication for the SSH server.

C9000 Series

Syntax

```
ip ssh password-authentication enable
```

To disable password-authentication, use the `no ip ssh password-authentication enable` command.

Parameters

enable	Enter the keyword `enable` to enable password-authentication for the SSH server.

Defaults

Enabled

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820t.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

With password authentication enabled, you can authenticate using the local, RADIUS, or TACACS+ password fallback order as configured.

ip ssh pub-key-file

Specify the file used for host-based authentication.

C9000 Series

Syntax `ip ssh pub-key-file {WORD}`

Parameters

WORD	Enter the file name for the host-based authentication.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information This command specifies the file used for the host-based authentication. The `creates/` file overwrites the `flash://ADMIN_DIR/ssh/knownhosts` file and deletes the user-specified file. Even though this command is a global configuration command, it does not appear in the running configuration because you only need to run this command once.

The file contains the OpenSSH-compatible public keys of the host for which host-based authentication is allowed. An example known host file format:

```
poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui+DWEc3cgYAcU5Lai1MU2ODrzhCwyDNp05tKBU3t
ReG1o8AxLi6+S4hyEMqHzkzBFNVqHzpQc
+Rs4p2urzV0F4pRKnaXdHf3Lk4D460HZRhhVrxqeNxPDpEn WIMPJi0ds= ashwani@poclab4
```

NOTE: For `rhostfile` and `pub-key-file`, the administrator must FTP the file to the chassis.

Example

```
Dell#conf
Dell(conf)# ip ssh pub-key-file flash://knownhosts
Dell(conf)#
```

Related Commands show ip ssh client-pub-keys — displays the client-public keys used for the host-based authentication.

ip ssh mac

Configure the list of MAC algorithms supported on both SSH client and SCP.

Syntax `ip ssh mac mac-list`

Parameters

mac *mac-list* Enter the keyword `mac` then a space-delimited list of message authentication code (MAC) algorithms supported by the SSH client. The following MAC algorithms are available.

When FIPS mode is enabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`

When FIPS mode is disabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-md5`
- `hmac-md5-96`

Defaults The default list of MAC algorithm is in the order as shown below:

When FIPS mode is enabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`

When FIPS mode is disabled:

- `hmac-sha2-256`
- `hmac-sha1`
- `hmac-sha1-96`
- `hmac-md5`
- `hmac-md5-96`

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.0)	Introduced on the S6100–ON, S6000, S6000–ON, S5000, S4810, S4820T, S3048–ON, S4048–ON, MXL, C9010, S3100 series, and Z9100-ON.

Usage Information

- You can select one or more MAC algorithms from the list.
- Client-supported MAC list gets preference over the server-supported MAC list in selecting the MAC algorithm for the SSH session.
- When the `MAC (-m)` option is used with the SSH CLI, it overrides the configured or default MAC list.
- When FIPS is enabled or disabled, the client MACs get default configuration.

ip ssh rekey

Configures the time rekey-interval or volume rekey-limit threshold at which to re-generate the SSH key during an SSH session.

C9000 Series

Syntax

`ip ssh rekey [time rekey-interval] [volume rekey-limit]`

To reset to the default, use `no ip ssh rekey [time rekey-interval] [volume rekey-limit]` command.

Parameters

time *minutes*	Enter the keywords `time` then the amount of time in minutes. The range is from 10 to 1440 minutes. The default is **60** minutes
volume *rekey-limit*	Enter the keywords **volume** then the amount of volume in megabytes. The range is from 1 to 4096 to megabytes. The default is **1024 megabytes**

Defaults

The default time is **60** minutes. The default volume is **1024** megabytes.

Command Modes

CONFIGURATION mode

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

ip ssh rhostsfile

Specify the rhost file used for host-based authorization.

C9000 Series

Syntax

`ip ssh rhostsfile {WORD}`

Parameters

WORD	Enter the rhost file name for the host-based authentication.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#conf
Dell(conf)# ip ssh rhostsfile flash://shosts
Dell(conf)#
```

Usage Information This command specifies the rhost file used for host-based authentication. This `creates/` file overwrites the `flash:/ADMIN_DIR/ssh/shosts` file and deletes the user-specified file. Even though this command is a global configuration command, it does not appear in the running configuration because you only need to run this command once.

This file contains hostnames and usernames, for which hosts and users, rhost-authentication can be allowed.

NOTE: For `rhostfile` and `pub-key-file`, the administrator must FTP the file to the switch.

ip ssh rsa-authentication (Config)

Enable RSA authentication for the SSHv2 server.

C9000 Series

Syntax `ip ssh rsa-authentication enable`

To disable RSA authentication, use the `no ip ssh rsa-authentication enable` command.

Parameters

enable	Enter the keyword `enable` to enable RSA authentication for the SSHv2 server.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information Enabling RSA authentication allows the user to log in without being prompted for a password. In addition, the OpenSSH compatible SSHv2 RSA public key must be added to the list of authorized keys (`ip ssh rsa-authentication my-authorized-keys device://filename` command).

Related Commands ip ssh rsa-authentication (EXEC) — adds keys for RSA authentication.

ip ssh rsa-authentication (EXEC)

Add keys for the RSA authentication.

C9000 Series

Syntax `ip ssh rsa-authentication {my-authorized-keys` *`WORD`*`}`

To delete the authorized keys, use the `no ip ssh rsa-authentication {my-authorized-keys}` command.

Parameters

my-authorized-keys *WORD*	Enter the keywords `my-authorized-keys` then the filename of the RSA authorized-keys.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

If you want to log in without being prompted for a password, log in through RSA authentication. To do that, first add the SSHv2 RSA public keys to the list of authorized keys. This command adds the specified RSA keys to the following file: `flash://ADMIN_DIR/ssh/authorized-keys-username` (where `username` is the user associated with this terminal).

NOTE: The `no` form of this command deletes the file `flash://ADMIN_DIR/ssh/ authorized-keys-username` file.

Related Commands

show ip ssh rsa-authentication — displays the RSA authorized keys.

ip ssh rsa-authentication (Config) — enables RSA authentication.

ip ssh server

Configure an SSH server. The SSH server is enabled by default.

C9000 Series

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

`ip ssh server {ciphers cipher-list} {enable | port port-number} [kex key-exchange-algorithm] [mac hmac-algorithm] [version {1 | 2}]`

To disable SSH server functions, use the `no ip ssh server {ciphers cipher-list} {enable | port port-number} [kex key-exchange-algorithm] [mac hmac-algorithm] [version {1 | 2}]` command.

Parameters

enable	Enter the key word `enable` to start the SSH server.
ciphers *cipher-list*	Enter the keyword `ciphers` and then a space-delimited list of ciphers that the SSH server supports. The following ciphers are available. • `3des-cbc` • `aes128-cbc`

- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

The default cipher list is used.

- 3des-cbc
- aes128-cbc
- aes192-cbc
- aes256-cbc
- aes128-ctr
- aes192-ctr
- aes256-ctr

mac *hmac-algorithm*

Enter the keyword `mac` then a space-delimited list of hash message authentication code (HMAC) algorithms supported by the SSH server for keying hashing for the message authentication.

The following HMAC algorithms are available:

- hmac-sha1
- hmac-sha1-96
- hmac-sha2-256

When FIPS is enabled, the default HMAC algorithm is `hmac-sha1-96`.

When FIPS is not enabled, the default HMAC algorithms are the following:

- hmac-md5
- hmac-md5-96
- hmac-sha1
- hmac-sha1-96
- hmac-sha2-256

kex *key-exchange-algorithm*

Enter the keyword `kex` and then a space-delimited list of key exchange algorithms supported by the SSH server.

The following key exchange algorithms are available:

- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1
- diffie-hellman-group14-sha1

When FIPS is enabled, the default key-exchange-algorithm is `diffie-hellman-group14-sha1`.

When FIPS is not enabled, the default key-exchange-algorithms are the following:

- diffie-hellman-group-exchange-sha1
- diffie-hellman-group1-sha1,

- `diffie-hellman-group14-sha1`

port *port-number* (OPTIONAL) Enter the keyword `port` then the port number of the listening port of the SSH server. The range is from 1 to 65535. The default is **22**.

[version {1 | 2}] (OPTIONAL) Enter the keyword `version` then the SSH version 1 or 2 to specify only SSHv1 or SSHv2.

NOTE: If you enable FIPS mode, you can only select version 2.

Defaults

- Default listening port is **22**.
- Default cipher list is 3des-cbc,aes128-cbc,aes192-cbc,aes256-cbc,aes128-ctr,aes192-ctr,aes256-ctr.
- When FIPS is enabled, the default is hmac-sha1-96.
- When FIPS is not enabled, the default is hmac-md5,hmac-md5-96,hmac-sha1,hmac-sha1-96,hmac-sha2-256.
- *When FIPS is enabled, the default is* diffie-hellman-group14-sha1.
- When FIPS is not enabled, the default is diffie-hellman-group-exchange-sha1,diffie-hellman-group1-sha1,diffie-hellman-group14-sha1.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced the `cipher`, `kex` and `mac` options on the Z9500.
9.5(0.0)	Introduced the `cipher`, `kex` and `mac` options on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information This command enables the SSH server and begins listening on a port. If a port is not specified, listening is on SSH default port 22.

Example

```
Dell# conf
Dell(conf)# ip ssh server port 45
Dell(conf)# ip ssh server enable
Dell#
```

Related Commands show ip ssh — displays the ssh information.

ip ssh server dns enable

Enable or disable the DNS in SSH server configuration to resolve hostname for host-based authenticatioin.

Syntax

```
ip ssh server dns enable
```

To disable the DNS in SSH server configuration, use the `no ip ssh server dns enable` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13.0.1	Introduced on the MXL, C9010, S3048–ON, S3100 series, S4810, S4820T, S4048–ON, S4048T-ON, S5000, S6000, S6000–ON, S6100–ON, S6010–ON, Z9500, Z9100–ON and FN-IOM.

Usage Information

To disable the DNS in SSH server configuration, use the `no ip ssh server dns enable` command.

ip ssh source-interface

Specifies an interface's IP address as the source IP address for an outgoing SSH connections.

C9000 Series

Syntax

```
ip ssh source-interface interface
```

To delete a source interface, use the `no ip ssh source-interface` command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16838.
- For the Null interface, enter the keywords `null 0`.
- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S-Series and Z9000.

Usage Information The `source-interface` *interface* attribute is applicable for both the `SSH client` as well as the `COPY` (SCP) commands. Using these attributes the client session tags an error to the user during run time, in case there is a mismatch between this command and the `ip ssh vrf` command.

Example

```
Dell(conf)#ip ssh source-interface tengigabitethernet 0/36
Dell(conf)#do ssh 10.10.10.2 -l admin
Dell(conf)#no ip ssh source-interface
```

show crypto

Display the public part of the SSH host-keys.

C9000 Series

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
show crypto key mypubkey {rsa | rsa1}
```

Parameters

Key	Enter the keyword `key` to display the host public key.
mypubkey	Enter the keyword `mypubkey` to display the host public key.
rsa	Enter the keyword `rsa` to display the host SSHv2 RSA public key.
rsa1	Enter the keyword `rsa1` to display the host SSHv1 RSA public key. **NOTE: If you enable FIPS mode, this parameter is not available.**

Defaults none

Command Modes EXEC

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

This command is useful if the remote SSH client implements Strict Host Key Checking. You can copy the host key to your list of known hosts.

Example

```
Dell#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAtzkZME/
e8V8smnXR22EJGQhCMkEOkuisa+ OILVoMYU1ZKGfj0W5BPCSvF/
x5ifqYFFwUzJNOcsJK7vjSsnmMhChF2YSvXlvTJ6h971F JAQlOsgd0ycpocsF
+DNLKfJnx7SAjhakFQMwG
g/g78ZkDT3Ydr8KKjfSI4Bg/WS8B740=

Dell#show crypto key mypubkey rsa1
1024 35
131060015480873398953257515397249657850072 2
064442949636740809356830889610203172266
798895675496676526500637962218977992760927 8
523638839223055081819166009928132616408
664345774602219229518903992966334579117374 22
474315537505016769296602737906014944 34
050000015179864425629613385774919236081 771341059533760063913083
Dell#
```

Related Commands

crypto key generate — generates the SSH keys.

show ip ssh

Display information about established SSH sessions.

C9000 Series

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
show ip ssh
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Updated the output to include `challenge-response-authentication` option.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell# show ip ssh
SSH server                : enabled.
SSH server version        : v1 and v2.
SSH server vrf            : default.
SSH server ciphers        : aes256-ctr, aes256-cbc, aes192-ctr, aes192-cbc,
aes128-ctr, aes128-cbc, 3des-cbc.
SSH server macs           : hmac-sha2-256, hmac-sha1, hmac-sha1-96, hmac-md5,
hmac-md5-96.
SSH server kex algorithms : diffie-hellman-group-exchange-sha1,diffie-hellman-
group1-sha1,diffie-hellman-group14-sha1.
Password Authentication   : enabled.
Hostbased Authentication  : disabled.
RSA       Authentication  : disabled.
Challenge Response Auth   : enabled.
   Vty          Encryption      HMAC            Remote IP
   2            aes128-cbc      hmac-md5        10.16.127.141
   4            aes128-cbc      hmac-md5        10.16.127.141
*  5            aes128-cbc      hmac-md5        10.16.127.141
Dell#
```

Related Commands

ip ssh server — configures an SSH server.

show ip ssh client-pub-keys — displays the client-public keys.

show ip ssh client-pub-keys

Display the client public keys used in host-based authentication.

C9000 Series

Syntax `show ip ssh client-pub-keys`

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information This command displays the contents of the `flash://ADMIN_DIRssh/knownhosts` file.

Example

```
Dell#show ip ssh client-pub-keys

poclab4,123.12.1.123 ssh-rsa AAAAB3NzaC1yc2EAAAABIwAAAIEAox/
QQp8xYhzOxn07yh4VGPAoUfgKoieTHO9G4sNV+ui
+DWEc3cgYAcU5Lai1MU2ODrzhCwyDNp05tKBU3tReG1
o8AxLi6+S4hyEMqHzkzBFNVqHzpQc
+Rs4p2urzV0F4pRKnaXdHf3Lk4D460HZRhhVrxqeNxPDpEnWIMPJi0
ds= ashwani@poclab4

Dell#
```

Related Commands ip ssh pub-key-file — configures the filename for the host-based authentication.

show ip ssh rsa-authentication

Display the authorized-keys for the RSA authentication.

C9000 Series

Syntax `show ip ssh rsa-authentication {my-authorized-keys}`

Parameters

my-authorized-keys Display the RSA authorized keys.

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information This command displays the contents of the `flash:/ADMIN_DIR/ssh/authorized-keys.username` file.

Example

```
Dell#show ip ssh rsa-authentication my-authorized-keys
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB17l4gFp4r2DRHI
vMc1VZd0Sg5GQxRV1y1X1JOMeO6Nd0WuYyzrQMM
4qJAoBwtneOXfLBcHF3V2hcMIqaZN+CRCnw/
zCMlnCf0+qVTd1oofsea5r09kS0xTp0CNfHXZ3NuGC
q9Ov33m9+U9tMwhS8vy8AVxdH4x4km3c3t5Jvc=
freedom@poclab4

Dell#
```

Related Commands ip ssh rsa-authentication (Config) — configures the RSA authorized keys.

ssh

Open an SSH connection specifying the hostname, username, encryption cipher, HMAC algorithm, port number, and version of the SSH client.

C9000 Series

Syntax

NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
ssh[vrf vrf-name] {hostname | ipv4 address | ipv6 address} [-c encryption
cipher | -l username | -m HMAC algorithm | -p port-number | -v {1 | 2}]
```

Parameters

vrf *vrf-name* (OPTIONAL) Enter the keyword `vrf` aand then the name of the VRF to specify the VRF used with the SSH session.

NOTE: The VRF configured using this command has a higher precedence than the VRF configured using the `ip ssh vrf vrf-name` command. If you do not configure a VRF using this command, then the SSH client uses the configured VRF (if any). If there is a mismatch between VRFs that are configured using the `ip ssh source-interface` command and the `ssh vrf vrf-name` command, then an error is reported.

hostname (OPTIONAL) Enter the IP address or the host name of the remote device.

vrf instance	(OPTIONAL) E-Series Only: Enter the keyword `vrf` then the VRF Instance name to open an SSH connection to that instance.
ipv4 address	(OPTIONAL) Enter the IP address in dotted decimal format A.B.C.D.
ipv6-address prefix-length	(OPTIONAL) Enter the IPv6 address in the x:x:x:x::x format then the prefix length in the /x format. The range is from /0 to /128. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
-c *encryption cipher*	Enable the “FIPS mode enable", this mode will support only v2 client. "no fips mode enable"(disable) will support v1 & v2 client. This comment is applicable for both ciphers & HMAC algorithms: • `3des-cbc` • `aes128-cbc` • `aes192-cbc` • `aes256-cbc` • `aes128-ctr` • `aes192-ctr` • `aes256-ctr`
-l *username*	(OPTIONAL) Enter the keyword `-l` then the user name used in this SSH session. The default is the user name of the user associated with the terminal.
-m *HMAC algorithm*	Enter one of the following HMAC algorithms to use. (For v2 clients only): "no fips mode enable"(disable) will support v1 & v2 client. • `hmac-sha1`: Force ssh to use hmac-sha1 HMAC algorithm. • `hmac-sha1-96`: Force ssh to use hmac-sha1-96 HMAC algorithm. • `hmac-md5`: Force ssh to use hmac-md5 HMAC algorithm. • `hmac-md5-96`: Force ssh to use hmac-md5-96 HMAC algorithm. • `hmac-sha2-256` : Force ssh to use hmac-sha2-256 HMAC algorithm.
-p *port-number*	(OPTIONAL) Enter the keyword `-p` then the port number. The range is from 1 to 65535. The default is **22**.
-v {1 | 2}	(OPTIONAL) Enter the keyword `-v` then the SSH version 1 or 2. The default is the version from the protocol negotiation.

Defaults

As shown in the *Parameters* section.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Removed the support for `hmac-sha2-256-96` algorithm.
9.9(0.0)	Introduced on the C9010.

Version	Description
9.5(0.1)	Added support for the following ciphers and HMAC alogorithms on the Z9000, S6000, S4820T, S4820T. • aes128-cbc • aes192-cbc • aes256-cbc • aes128-ctr • aes192-ctr • aes256-ctr • hmac-sha2-256 • hmac-sha2-256-96
9.4(0.0)	Added support for VRF.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.12.0	Added support for the `-c` and `-m` parameters on the S4810.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Added IPv6 support. Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information Dell Networking OS supports both inbound and outbound SSH sessions using IPv4 or IPv6 addressing. Inbound SSH supports accessing the system through the management interface as well as through a physical Layer 3 interface.

Example

```
Dell#ssh 10.11.8.12 ?
-c        Encryption cipher to use (for v2 clients only)
-l        User name option
-m        HMAC algorithm to use (for v2 clients only)
-p        SSH server port option (default 22)
-v        SSH protocol version
<cr>

Dell#ssh 10.11.8.12 -c ?
3des-cbc  Force ssh to use 3des-cbc encryption cipher

Dell#ssh 10.11.8.12 -m ?
hmac-sha1    Force ssh to use hmac-sha1 HMAC algorithm
hmac-sha1-96 Force ssh to use hmac-sha1-96 HMAC algorithm
hmac-md5     Force ssh to use hmac-md5 HMAC algorithm
hmac-md5-96  Force ssh to use hmac-md5-96 HMAC algorithm
Dell#ssh vrf vrf1 10.10.10.2 -l admin
```

Secure DHCP Commands

DHCP as defined by RFC 2131 provides no authentication or security mechanisms. Secure DHCP is a suite of features that protects networks that use dynamic address allocation from spoofing and attacks.

clear ip dhcp snooping

Clear the DHCP binding table.

C9000 Series

Syntax `clear ip dhcp snooping binding`

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Related Commands show ip dhcp snooping — displays the contents of the DHCP binding table.

ip dhcp snooping

Enable DHCP Snooping globally.

C9000 Series

Syntax `[no] ip dhcp snooping`

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information When enabled, no learning takes place until you enable snooping on a VLAN. After disabling DHCP Snooping, the binding table is deleted and Option 82, IP Source Guard, and Dynamic ARP Inspection are disabled.

Related Commands ip dhcp snooping vlan — enables DHCP Snooping on one or more VLANs.

ip dhcp snooping binding

Create a static entry in the DHCP binding table.

C9000 Series

Syntax `[no] ip dhcp snooping binding mac address vlan-id vlan-id ip ip-address interface type slot/port lease number`

Parameters

mac *address*	Enter the keyword `mac` then the MAC address of the host to which the server is leasing the IP address.
vlan-id *vlan-id*	Enter the keywords `vlan-id` then the VLAN to which the host belongs. The range is from 2 to 4094.
ip *ip-address*	Enter the keyword `ip` then the IP address that the server is leasing.
interface *type*	Enter the keyword `interface` then the type of interface to which the host is connected. • For a 10-Gigabit Ethernet interface, enter the keyword `tengigabitethernet`. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE`.
slot/port	Enter the slot and port number of the interface.
lease *time*	Enter the keyword `lease` then the amount of time the IP address is leased. The range is from 1 to 4294967295.

Defaults none

Command Modes
- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Related Commands show ip dhcp snooping — displays the contents of the DHCP binding table.

ip dhcp snooping database

Delay writing the binding table for a specified time.

C9000 Series

Syntax `ip dhcp snooping database write-delay minutes`

Parameters

minutes	The range is from 5 to 21600.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping database renew

Renew the binding table.

C9000 Series

Syntax	`ip dhcp snooping database renew`
Defaults	none
Command Modes	• EXEC • EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping trust

Configure an interface as trusted.

C9000 Series

Syntax	`[no] ip dhcp snooping trust`
Defaults	Untrusted
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp source-address-validation

Enable IP source guard.

C9000 Series

Syntax `[no] ip dhcp source-address-validation`

Defaults Disabled.

Command Modes INTERFACE

INTERFACE (BATCH Mode)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

C9000 Series

Syntax `[no] ip dhcp snooping vlan` *name*

Parameters

name — Enter the name of a VLAN on which to enable DHCP Snooping.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Usage Information When enabled, the system begins creating entries in the binding table for the specified VLANs.

NOTE: Learning only happens if there is a trusted port in the VLAN.

Related Commands ip dhcp snooping trust — configures an interface as trusted.

show ip dhcp snooping

Display the contents of the DHCP binding table.

C9000 Series

Syntax

```
show ip dhcp snooping binding
```

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the C-Series and S-Series.

Related Commands clear ip dhcp snooping — clears the contents of the DHCP binding table.

ICMP Vulnerabilities

The internet control message protocol (ICMP) is a network-layer internet protocol that provides message packets to report errors and other information regarding IP packet processing back to the source. Dell Networking OS mainly addresses the following ICMP vulnerabilities:

- ICMP Mask Reply
- ICMP Timestamp Request
- ICMP Replies
- IP ID Values Randomness

You can configure the Dell Networking OS to drop ICMP reply messages. When you configure the `drop icmp` command, the system drops the ICMP reply messages from the front end and management interfaces. By default, the Dell Networking OS responds to all the ICMP messages. You can configure the Dell Networking OS to suppress the following ICMPv4 and ICMPv6 message types:

Table 11. Suppressed ICMPv4 message types

ICMPv4 Message Types
Echo reply (0)
All sub types of destination unreachable (3)
Source quench (4)
Redirect (5)
Router advertisement (9)
Router solicitation (10)
Time exceeded (11)
IP header bad (12)
Timestamp request (13)
Timestamp reply (14)
Information request (15)
Information reply (16)
Address mask request (17)
Address mask reply (18)

NOTE: The Dell Networking OS does not suppress the ICMPv4 message type `Echo request (8).`

Table 12. Suppressed ICMPv6 message types

ICMPv6 Message Types
Destination unreachable (1)
Time exceeded (3)
IPv6 header bad (4)
Echo reply (129)
Who are you request (139)
Who are you reply (140)
Mtrace response (200)
Mtrace messages (201)

NOTE:
The Dell Networking OS does not suppress the following ICMPv6 message types:

- Packet too big (2)
- Echo request (128)
- Multicast listener query (130)
- Multicast listener report (131)
- Multicast listener done (132)
- Router solicitation (133)
- Router advertisement (134)
- Neighbor solicitation (135)
- Neighbor advertisement (136)
- Redirect (137)
- Router renumbering (138)
- MLD v2 listener report (143)
- Duplicate Address Request (157)
- Duplicate Address Confirmation (158)

drop icmp

Drops the ICMPv4 and ICMPv6 packets.

Syntax `drop {icmp | icmp6}`

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other Platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11.0.0	Introduced on the S4810, S4820T, S3048–ON, S3100 Series, S4048–ON, S5000, S6000, S6000–ON, Z9500, Z9100–ON, S6100–ON, S6010–ON, S4048T–ON, C9000, and MXL.

Usage Information

When the `drop icmp` feature is configured, the system drops the ICMP reply messages on the front end and management interfaces. By default, the Dell Networking OS responds to all the ICMP messages.

NOTE: There is no separate CLI to enable IP ID randomness. By default, the IP ID in the kernel is randomized.

For more information on the ICMP message types, see the ICMP Commands section.

System Security Commands

The following section lists the system security commands.

boot-access password

Set a password for the boot loader.

Syntax

`boot-access password [encryption-type] boot-password`

To remove the GRUB access password, use the `no boot-access password` command.

Parameters

encryption-type	(OPTIONAL) Enter an encryption type for the boot password. • 0 directs the system to store the password as clear text. • 7 directs the system to store the password with a dynamic salt.
boot-password	Enter the boot access password.

Defaults

None

Command Modes

CONFIGURATION.

Command History

Version	Description
9.13(0.0)	Introduced on the S3048–ON, S4048–ON, S4048T-ON, S6000–ON, S6010–ON, S6100–ON, and Z9100–ON.

Usage Information

If you enable the boot access password, the system prompts for a password when you access the GRUB interface.

When you configure the boot access password, ensure that your password meets the following criteria:

- A minimum of eight characters in length
- A minimum of one lower case letter (a to z)
- A minimum of one upper case letter (A to Z)
- A minimum of one numeric character (0 to 9)
- A minimum of one special character including a space (" !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~")

If your password does not meet the criteria, the system does not accept your password.

When you upgrade the Dell EMC Networking OS image, ensure that you upgrade the boot loader.

CAUTION: After configuring the boot access password, save it to a secure location. If you forget it, you will not be able to access the options in the startup menu. If you forget both the boot access password and the enable password, the system may become inaccessible.

Example

```
DellEMC(conf)#boot-access password 7 Hg$7^5HMoiY%
    ********************************************************************
    *  Warning - boot-access password will enable password protection in  *
    *  GRUB. Keep it safe. Forgetting this password and the CLI password  *
    *  may result in switch becoming inaccessible.                        *
    ********************************************************************

Do you want to configure boot-access password? Proceed [yes/no]:yes
DellEMC(conf)#
```

generate hash

Generate a hash checksum for the given file or the startup configuration using the MD5, SHA1, or SHA256 algorithm.

Syntax

```
generate hash {md5 | sha1 | sha256} {flash://filename | startup-config}
```

Parameters

md5 | sha1 | sha256	Enter the keyword `md5`, `sha1`, or `sha256` to generate .
flash://*filename*	Enter the keyword `flash:` and enter the filename to generate the hash checksum for any file in the flash drive using the MD5, SHA1, or SHA256 algorithm.
startup-config	Enter the keyword `shartup-config` to generate the hash checksum for the startup configuration using the MD5, SHA1, or SHA256 algorithm.

Defaults

None

Command Modes

EXEC Privilege

Command History

Version	Description
9.13(0.0)	Introduced on the S3100 series, S3048–ON, S4048–ON, S4048T-ON, S5000, S6000, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, Z9500, C9010, MXL, and FN-IOM.

Usage Information

Use the `generate hash` command to generate a hash checksum for your startup configuration, and use the hash to verify using the `verified boot hash` command.

Example

```
DellEMC#generate hash md5 startup-config
MD5SUM(/f10/flash/startup-config) : f81812a64eea202c5b2ef782639bafc3
```

root-access password

Configure the root access password.

Syntax

```
root-access password [encryption-type] root-password
```

To reset to the default password, use the `no root-access password` command.

Parameters

encryption-type	(OPTIONAL) Enter an encryption type for the root password that you enter. • 0 directs the system to store the password as clear text. • 7 directs the system to store the password with a dynamic salt. • 9 directs the system to encrypt the clear text password and store the encrypted password in an inaccessible location.
root-password	Enter the root password.

Defaults Not configured

Command Modes CONFIGURATION

Command History

Version	Description
9.13(0.0)	Introduced on the S3100 series, S3048–ON, S4048–ON, S4048T-ON, S5000, S6000, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, Z9500, C9010, MXL, and FN-IOM.

Usage Information

If you configure the `secure-cli` command on the system, the Dell EMC Networking OS resets any previously-configured root access password to the default root password without displaying any warning message. With the `secure-cli` command enabled on the system, the CONFIGURATION mode does not display the `root access password` option.

When you configure the root access password, ensure that your password meets the following criteria:

- A minimum of eight characters in length
- A minimum of one lower case letter (a to z)
- A minimum of one upper case letter (A to Z)
- A minimum of one numeric character (0 to 9)
- A minimum of one special character including a space (" !"#$%&'()*+,-./:;<=>?@[\]^_`{|}~")

If your password does not meet the criteria, the system does not accept your password.

If you use encryption type 9, the system stores the clear text password in an inaccessible location on the system. The `show running-configuration` command does not display the password. This configuration is not portable between different systems.

Example

```
DellEMC)# show running-config  | g root
root-access password 7
f4dc0cb9787722dd1084d17f417f164cc7f730d4f03d4f0215294cbd899614e3
```

verified boot hash

Verify and store the hash value of the startup configuration.

Syntax `verified boot hash startup-config` *`hash value`*

Parameters

startup-config	Enter the keyword `startup-config` and then the hash value for the startup configuration. You can get the hash value for the startup configuration using the `generate hash` command.

	hash value	Enter the MD5, SHA1, or SHA256 hash.

Defaults None

Command Modes EXEC Privilege

Command History

Version	Description
9.13(0.0)	Introduced on the S3100 series, S3048–ON, S4048–ON, S4048T-ON, S5000, S6000, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, Z9500, C9010, MXL, and FN-IOM.

Usage Information Dell EMC Networking OS supports MD5, SHA1, and SHA256.

Example

```
DellEMC# verified boot hash system-image A: 619A8C1B7A2BC9692A221E2151B9DA9E
```

verified startup-config

Enable hash validation for the startup configuration during system startup.

Syntax

```
verified startup-config
```

To disable hash validation for the startup configuration, use the `no verified startup-config` command.

Defaults Not configured

Command Modes CONFIGURATION

Command History

Version	Description
9.13(0.0)	Introduced on the S3100 series, S3048–ON, S4048–ON, S4048T-ON, S5000, S6000, S6000–ON, S6010–ON, S6100–ON, Z9100–ON, Z9500, C9010, MXL, and FN-IOM.

Example

```
DellEMC(config)# verified startup-config
```

54

Service Provider Bridging

Service provider bridging is composed of virtual local area network (VLAN) Stacking, Layer 2 Protocol Tunneling, and Provider Backbone Bridging as described in the *Dell Networking OS Configuration Guide Service Provider Bridging* chapter.

This chapter includes command line information (CLI) for the Dell Networking operating software Layer 2 Protocol Tunneling (L2PT). L2PT enables protocols to tunnel through an 802.1q tunnel.

For more information, refer to VLAN Stacking, Spanning Tree Protocol (STP), and GARP VLAN Registration (GVRP).

Important Points to Remember

- L2PT is enabled at the interface VLAN-Stack VLAN level. For more information about Stackable VLAN (VLAN-Stacking) commands, refer to VLAN Stacking.
- The default behavior is to disable protocol packet tunneling through the 802.1q tunnel.
- Rate-limiting is required to protect against bridge protocol data units (BPDU) attacks.
- A port channel (including through link aggregation control protocol [LACP]) can be configured as a VLAN-Stack access or trunk port.
- Address resolution protocol (ARP) packets work as expected across the tunnel.
- Far-end failure detection (FEFD) works the same as with Layer 2 links.
- Protocols that use Multicast MAC addresses (for example, open shortest path first [OSPF]) work as expected and carry over to the other end of the VLAN-Stack VLAN.

Topics:

- debug protocol-tunnel
- protocol-tunnel
- protocol-tunnel destination-mac
- protocol-tunnel enable
- protocol-tunnel rate-limit
- show protocol-tunnel

debug protocol-tunnel

Enable debugging to ensure incoming packets are received and rewritten to a new MAC address.

C9000 Series

Syntax

```
debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]
```

To disable debugging, use the `no debug protocol-tunnel interface {in | out | both} [vlan vlan-id] [count value]` command.

Parameters

interface Enter one of the following interfaces and slot/port information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

in | out | both Enter the keyword `in`, `out`, or `both` to debug incoming interfaces, outgoing interfaces, or both incoming and outgoing interfaces.

vlan *vlan-id* Enter the keyword `vlan` then the VLAN ID. The range is from 1 to 4094.

count *value* Enter the keyword `count` then the number of debug outputs. The range is from 1 to 100.

Defaults Debug disabled.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series, E-Series, and E-Series ExaScale.
7.4.1.0	Introduced

protocol-tunnel

Enable protocol tunneling on a stacked (Q-in-Q) VLAN for specified protocol packets.

C9000 Series

Syntax `protocol-tunnel {rate-limit rate| stp}`

To disable protocol tunneling for a Layer 2 protocol, use the `no protocol-tunnel` command.

Parameters

rate-limit *rate* Enter the keyword `rate-limit` followed by a number for the rate-limit for tunneled packets on the VMAN. The range is from 64 to 320.

stp Enter the keyword `stp` to enable protocol tunneling on a spanning tree, including STP, MSTP, RSTP, and PVST.

Defaults none

Command Modes CONF-IF-VLAN

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.5.1.1	Added support for `802.1X`, `E-LMI`, `GMRP`, `GVRP`, `LLDP`, `LACP`, `MMRP`, `MVRP`, and `OAM 802.3ah` protocol traffic to the E-Series ExaScale.
8.2.1.0	Introduced on the C-Series, E-Series, and E-Series ExaScale.
7.4.1.0	Introduced

Example

```
Dell#conf
Dell(conf)#interface vlan 2
Dell(conf-if-vl-2)#vlan-stack compatible
Dell(conf-if-vl-2)#member Te 1/2-3
Dell(conf-if-vl-2)#protocol-tunnel stp
Dell(conf-if-vl-2)#protocol-tunnel enable
```

Related Command show protocol-tunnel — displays tunneling information for all VLANs.

protocol-tunnel destination-mac

Overwrite the BPDU destination MAC address with a specific value.

C9000 Series

Syntax `protocol-tunnel destination-mac` *`xstp address`*

Parameters

stp	Change the default destination MAC address used for L2PT to another value.

Defaults The default destination MAC is 01:01:e8:00:00:00.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series, and S-Series.
7.4.1.0	Introduced

Usage Information When you enable VLAN-Stacking, no protocol packets are tunneled.

Related Command show protocol-tunnel — displays tunneling information for all VLANs.

protocol-tunnel enable

Enable protocol tunneling globally on the system.

C9000 Series

Syntax `protocol-tunnel enable`

To disable protocol tunneling, use the `no protocol-tunnel enable` command.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.4.1.0	Introduced

Usage Information The system must have the default CAM profile with the default microcode before you enable L2PT.

protocol-tunnel rate-limit

Enable traffic rate limiting per box.

C9000 Series

Syntax

```
protocol-tunnel rate-limit rate
```

To reset the rate limit to the default, use the `no protocol-tunnel rate-limit rate` command.

Parameters

rate	Enter the rate in frames per second. The range is from 64 to 320 Kbps.

Defaults

no default rate-limit.

Command Modes

INTERFACE VLAN

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series, E-Series TeraScale, and E-Series ExaScale. Maximum rate limit on E-Series reduced from 4000 to 3000.
7.4.1.0	Introduced

Example

```
Dell(conf)#interface vlan 4001
Dell(conf-if-vl-4001-stack)#protocol-tunnel rate-limit 100
```

Related Commands

show protocol-tunnel — displays tunneling information for all VLANs.

show running-config — displays the current configuration.

show protocol-tunnel

Display protocol tunnel information for all or a specified VLAN-Stack VLAN.

C9000 Series

Syntax

```
show protocol-tunnel [vlan vlan-id]
```

Parameters

vlan *vlan-id*	(OPTIONAL) Enter the keyword `vlan` then the VLAN ID to display information for the one VLAN. The range is from 1 to 4094.

Defaults

none

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series, E-Series and E-Series ExaScale.
7.4.1.0	Introduced

Example

```
Dell#show protocol-tunnel
VLAN  Protocols    Rate-limit(Kbps)    Interface
4001  STP,PVST     -                   Te 1/17 Te 1/19
4002  STP,PVST     -                   Te 1/16 Te 1/18
Dell#

Dell#show protocol-tunnel vlan 4001
VLAN  Protocols    Rate-limit(Kbps)    Interface
4001  STP,PVST     -                   Te 1/17 Te 1/19
```

Example (Specific VLAN)

```
Dell#show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface  Vlan  Protocol(s)
Te1/2      2     STP, PVST
Dell#
```

Related Commands

show running-config — displays the current configuration.

55

sFlow

The Dell Networking operating software (OS) supports sFlow commands on Dell Networking OS.

Dell Networking operating software sFlow monitoring system includes an sFlow Agent and an sFlow Collector.

- The sFlow Agent combines the flow samples and interface counters into sFlow datagrams and forwards them to the sFlow Collector.
- The sFlow Collector analyses the sFlow Datagrams received from the different devices and produces a network-wide view of traffic flows.

Important Points to Remember

- Dell Networking recommends that the sFlow Collector be connected to the Dell Networking chassis through a line card port rather than the route processor module (RPM) Management Ethernet port.
- Dell Networking operating software exports all sFlow packets to the sFlow Collector. A small sampling rate can equate to many exported packets. A backoff mechanism is automatically applied to reduce this amount. Some sampled packets may be dropped when the exported packet rate is high and the backoff mechanism is about to or is starting to take effect. The dropEvent counter, in the sFlow packet, is always zero.
- sFlow sampling is done on a per-port basis.
- Community list and local preference fields are not filled up in the extended gateway element in the sFlow datagram.
- The 802.1P source priority field is not filled up in the extended switch element in the sFlow datagram.
- Only Destination and Destination Peer AS numbers are packed in the dst-as-path field in the extended gateway element.
- If the packet being sampled is redirected using policy-based routing (PBR), the sFlow datagram may contain incorrect extended gateway/router information.
- sFlow does not support packing extended information for IPv6 packets. Only the first 128 bytes of the IPv6 packet is shipped in the datagram.
- The source virtual local area network (VLAN) field in the extended switch element is not packed if there is a routed packet.
- The destination VLAN field in the extended switch element is not packed if there is a multicast packet.
- The sFlow sampling functionality is supported only for egress traffic and not for ingress traffic.
- The maximum number of packets that can be sampled and processed per second is:
  - 7500 packets when no extended information packing is enabled.
  - 7500 packets when only extended-switch information packing is enabled (refer to sflow extended-switch enable).
  - The outputPort field may not filled correctly on PE port sampled packets.

Topics:

- sflow collector
- sflow enable (Global)
- sflow enable (Interface)
- sflow ingress-enable
- sflow extended-switch enable
- sflow max-header-size extended
- sflow polling-interval (Global)
- sflow polling-interval (Interface)
- sflow sample-rate (Global)
- sflow sample-rate (Interface)

- show sflow
- show sflow linecard

sflow collector

Configure a collector device to which sFlow datagrams are forwarded.

C9000 Series

Syntax

`sflow collector {ip-address | ipv6-address} agent-addr {ip-address | ipv6-address} [number [max-datagram-size number]] | [max-datagram-size number] [vrf management]`

To delete a configured collector, use the `no sflow collector {ip-address | ipv6-address} agent-addr {ipv4-address | ipv6-address} [number [max-datagram-size number]] | [max-datagram-size number] [vrf management]` command.

Parameters

sflow collector *ip-address* | *ipv6-address*	Enter the IP address of the collector in dotted decimal format for IPv4 or x:x:x:x::x format for IPv6. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
agent-addr *ip-address* | *ipv6-address*	Enter the keyword `agent-addr` followed by the sFlow agent IP address in dotted decimal format for IPv4 or x:x:x:x::x format for IPv6. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
number	(OPTIONAL) Enter the user datagram protocol (UDP) port number. The range is from 0 to 65535. The default is 6343.
max-datagram-size *number*	(OPTIONAL) Enter the keyword max-datagram-size then the size number in bytes. The range is from 400 to 1500. The default is **1400**.
vrf management	(OPTIONAL) Enter the keyword `vrf` followed by the keyword `management` to configure the collector device corresponding to the default VRF and the management VRF respectively.

Defaults

Not configured.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.

Version	Description
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.3	Added support for IPv6 sFlow collectors and agents on the E-series TeraScale, C-Series, and S-Series.
8.4.1.1	Added support for IPv6 sFlow collectors and agents on the E-series ExaScale.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.5.1.0	Expanded the `no` form of the command to mirror the syntax used to configure.
6.2.1.1	Introduced on the E-Series.

Usage Information

You can configure up to two sFlow collectors (IPv4 or IPv6). If two collectors are configured, traffic samples are sent to both.

The sFlow agent address is carried in a field in SFlow packets and is used by the collector to identify the sFlow agent.

In sFlow, the agent address is a single invariant IPv4 or IPv6 address used to identify the agent to the collector. It is usually assigned the address of a loopback interface on the agent, which provides invariance. The agent address is carried as a field in the payload of the sFlow packets.

As part of the sFlow-MIB, if the SNMP request originates from a configured collector, Dell Networking OS returns the corresponding configured agent IP in the MIB requests. Dell Networking OS checks to ensure that two entries are not configured for the same collector IP with a different agent IP. Should that happen, Dell Networking OS generates the following error: `%Error: Different agent-addr attempted for an existing collector`.

Use this command in Configuration Terminal Batch mode to configure the sFlow collectors in a dual-homing setup.

Example

```
Dell(conf)#sflow collector 10.1.1.25 agent-addr 10.1.1.10 vrf management
```

sflow enable (Global)

Enable sFlow globally.

C9000 Series

Syntax

```
sflow enable
```

To disable sFlow, use the `no sflow enable` command.

Defaults

Disabled.

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

sFlow is disabled by default. In addition to this command, sFlow needs to be enable on individual interfaces where sFlow sampling is desired.

Use this command in Configuration Terminal Batch mode to enable sFlow in a dual-homing setup.

sflow enable (Interface)

Enable sFlow on interfaces.

C9000 Series

Syntax `sflow enable`

To disable sFlow, use the `no sflow enable` command.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information When you enable sFlow on an interface, flow sampling is done on any traffic going out of the interface.

NOTE: After a physical port is a member of a LAG, it inherits the sFlow configuration from the LAG port.

sflow ingress-enable

Enable sFlow ingress on interfaces.

C9000 Series

Syntax `sflow ingress-enable`

To disable sFlow, use the `no sflow ingress enable` command.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Introduced on the S-Series, Z-Series, and MXL switch.

Usage Information When you enable ingress sFlow on an interface, flow sampling is done on any incoming traffic.

NOTE: After a physical port is a member of a LAG, it inherits the sFlow configuration from the LAG port.

Related Commands sflow enable (Global) — turns sFlow globally.

sflow extended-switch enable

Enable packing information on a switch only.

C9000 Series

Syntax `sflow extended-switch enable`

To disable packing information, use the `no sflow extended-switch [enable]` command.

Parameters

enable	Enter the keyword `enable` to enable global extended information.

Defaults Disabled.

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0P5)	Introduced on the S4048-ON.

Version	Description
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

Dell Networking OS enhances the sflow implementation for real time traffic analysis on the E-Series to provide extended gateway information in cases where the destination IP addresses are learned by different routing protocols and for cases where the destination is reachable over ECMP.

Use this command in Configuration Terminal Batch mode to enable the packing information in a dual-homing setup.

Related Commands

show sflow — displays the sFlow configuration.

sflow max-header-size extended

Set the maximum header size of a packet to 256 bytes.

C9000 Series

Syntax

```
sflow max-header-size extended
```

To reset the maximum header size of a packet, use the `[no] sflow max-header-size extended` command.

Parameters

extended	Enter the keyword `extended` to copy 256 bytes from the sample packets to sFlow datagram.

Defaults

128 bytes

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Introduced on the S Series and Z Series switches.

Example

```
Dell(conf)#sflow max-header-size extended
```

sflow polling-interval (Global)

Set the sFlow polling interval at a global level.

C9000 Series

Syntax

`sflow polling-interval` *`interval value`*

To return to the default, use the `no sflow polling-interval` *`interval`* command.

Parameters

interval value	Enter the interval value in seconds. The range is from 15 to 86400 seconds. The default is **20 seconds**.

Defaults

20 seconds

Command Modes

CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

The polling interval for an interface is the maximum number of seconds between successive samples of counters sent to the collector. This command changes the global default counter polling (20 seconds) interval. You can configure an interface to use a different polling interval.

Use this command in Configuration Terminal Batch mode to set the sFlow polling interval in a dual-homing setup.

Related Commands

sflow polling-interval (Interface) — sets the polling interval for an interface.

sflow polling-interval (Interface)

Set the sFlow polling interval at an interface (overrides the global-level setting.)

C9000 Series

Syntax

`sflow polling-interval` *`interval value`*

To return to the default, use the `no sflow polling-interval` *`interval`* command.

Parameters

interval value	Enter the interval value in seconds. The range is from 15 to 86400 seconds. The default is **the global counter polling interval**.

Defaults

The same value as the current global default counter polling interval.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.

Version	Description
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information This command sets the counter polling interval for an interface.

Related Commands sflow polling-interval (Global) — globally sets the polling interval.

sflow sample-rate (Global)

Change the global default sampling rate.

C9000 Series

Syntax `sflow sample-rate value`

To return to the default sampling rate, use the `no sflow sample-rate` command.

Parameters

value	Enter the sampling rate value. For the C-Series and S-Series, the range is from 256 to 8388608 packets Enter values in powers of 2 only; for example, 4096, 8192, 16384, and so on. The default is **32768 packets**.

Defaults **32768 packets**

Command Modes CONFIGURATION

CONFIGURATION TERMINAL BATCH

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.10(0.0)	Introduced the Configuration Terminal Batch mode on C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
7.4.1.0	Introduced on the E-Series.

Usage Information

Sample-rate is the average number of packets skipped before the sample is taken. This command changes the global default sampling rate. You can configure an interface to use a different sampling rate than the global sampling rate. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power of 2 value. Select one of these two packet numbers and re-enter the command.

Use this command in Configuration Terminal Batch mode to change the sampling rate in a dual-homing setup.

Related Commands

sflow sample-rate (Interface) — changes the interface sampling rate.

sflow sample-rate (Interface)

Change the interface default sampling rate.

C9000 Series

Syntax

```
sflow sample-rate value
```

To return to the default sampling rate, use the `no sflow sample-rate` command.

Parameters

value	Enter the sampling rate value. For the C-Series and S-Series, the range is from 256 to 8388608 packets. Enter values in powers of 2 only; for example, 4096, 8192, 16384, etc. The default is **32768** packets.

Defaults

The Global default sampling.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information This command changes the sampling rate for an interface. By default, the sampling rate of an interface is set to the same value as the current global default sampling rate if port is operationally down, otherwise sampling rate changes based on port line speed. If the value entered is not a correct power of 2, the command generates an error message with the previous and next power-of-2 value. Select one of these two number and re-enter the command.

Related Commands sflow sample-rate (Global) — changes the sampling rate globally.

show sflow

Display the current sFlow configuration.

Syntax `show sflow [interface]`

Parameters

interface (OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information.
- For a port channel interface, enter the keywords `port-channel` then a number.
- For a 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` then the slot/port information.
- For a port extender Gigabit Ethernet interface, enter the keyword `peGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the *stack-unit* unit-number range is from 0 to 7; and the *port-id* range is from 1 to 48.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255;

the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The dropEvent counter (sFlow samples dropped due to sub-sampling) shown in the following example always displays a value of zero.

Example

show sflow linecard

Display sFlow information for a line card.

C9000 Series

Syntax `show sflow linecard slot-id`

Parameters

slot number	Enter a slot number to view information on the line-card ports in that slot. The range of Z9500 slot IDs is from 0 to 2.

Command Modes

- EXEC

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced on S-Series Stacking.
8.1.1.0	Introduced on the E-Series ExaScale.
7.7.1.0	Introduced on the S-Series.
7.6.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell# show sflow linecard 0
Linecard 0
  Samples rcvd from h/w            :0
  Total UDP packets exported       :0
  UDP packets exported via RPM     :0
  UDP packets dropped              :0

Dell# show sflow linecard 1
Linecard 1
  Samples rcvd from h/w            :0
  Total UDP packets exported       :0
  UDP packets exported via RPM     :0
  UDP packets dropped              :0

Dell# show sflow linecard 2
Linecard 2
  Samples rcvd from h/w            :0
  Total UDP packets exported       :0
  UDP packets exported via RPM     :0
  UDP packets dropped              :0
Dell#
```

56

Simple Network Management Protocol (SNMP) and Syslog

This chapter contains commands to configure and monitor the simple network management protocol (SNMP) v1/v2/v3 and Syslog.

The chapter contains the following sections:

- SNMP Commands
- Syslog Commands

Topics:

- SNMP Commands
- Syslog Commands

SNMP Commands

The following SNMP commands are available in the Dell Networking operating software.

The simple network management protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements. The system supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. The system sends SNMP traps, which are messages informing an SNMP management system about the network. The system supports up to 16 SNMP trap receivers.

Important Points to Remember

- Typically, 5-second timeout and 3-second retry values on an SNMP server are sufficient for both LAN and WAN applications. If you experience a timeout with these values, the recommended best practice on Dell Networking switches (to accommodate their high port density) is to increase the timeout and retry values on your SNMP server to the following:
  - SNMP Timeout — greater than 3 seconds.
  - SNMP Retry count — greater than 2 seconds.
- If you want to query an E-Series switch using SNMP v1/v2/v3 with an IPv6 address, configure the IPv6 address on a non-management port on the switch.
- If you want to send SNMP v1/v2/v3 traps from an E-Series using an IPv6 address, use a non-management port.
- SNMP v3 informs are not currently supported with IPv6 addresses.
- If you are using access control lists (ACLs) in an SNMP v3 configuration, group ACL overrides user ACL if the user is part of that group.
- SNMP operations are not supported on a virtual local area network (VLAN).

show snmp

Display the status of SNMP network elements.

C9000 Series

Syntax

```
show snmp
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
Dell#show snmp
  32685 SNMP packets input
      0 Bad SNMP version errors
      0 Unknown community name
      0 Illegal operation for community name supplied
      0 Encoding errors
  96988 Number of requested variables
      0 Number of altered variables
  31681 Get-request PDUs
    968 Get-next PDUs
      0 Set-request PDUs
  61727 SNMP packets output
      0 Too big errors (Maximum packet size 1500)
      9 No such name errors
      0 Bad values errors
      0 General errors
  32649 Response PDUs
  29078 Trap PDUs
Dell#
```

Related Commands

snmp-server community — enables the SNMP and set community string.

show snmp engineID

Display the identification of the local SNMP engine and all remote engines that are configured on the router.

C9000 Series

Syntax

```
show snmp engineID
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
Dell#show snmp engineID
Local SNMP engineID: 0000178B02000001E80214A8
Remote Engine ID        IP-addr      Port
80001F88043132333435    172.31.1.3   5009
80001F88043938373635    172.31.1.3   5008

Dell#
```

Related Commands

snmp-server engineID — configures local and remote SNMP engines on the router.

show snmp group

Display the group name, security model, status, and storage type of each group.

C9000 Series

Syntax

```
show snmp group
```

Command Modes

- EXEC

- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

The following Example displays a group named *ngroup*. The *ngroup* has a security model of version 3 (v3) with authentication (`auth`), the read and notify name is *nview* with no write view name specified, and finally the row status is active.

Example

```
Dell#show snmp group

groupname: ngroup          security model: v3 auth
readview : nview           writeview: no write view specified
notifyview: nview
row status: active

Dell#
```

Related Commands

snmp-server group — configures an SNMP server group.

show snmp supported-mibs

Display the list of SNMP MIBs supported by the platform.

Syntax

```
show snmp supported-mibs
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the C9010, FN-IOM, MIOA, MXL, S3048–ON, S3100, S4048–ON, S4048T-ON, S5048F-ON, S6000, S6000–ON, S6010–ON, S6100–ON and Z9100–ON.

Example

```
DellEMC#show snmp supported-mibs
MIB                                          OID
------------------------------------------------------------
```

```
RFC1155-SMI                              -
RFC-1212                                 -
SNMPv2-SMI                               -
SNMPv2-TC                                -
SNMPv2-CONF                              -
INET-ADDRESS-MIB                         -
IANAifType-MIB                           -
IANA-ADDRESS-FAMILY-NUMBERS-MIB          -
IANA-RTPROTO-MIB                         -
IPV6-FLOW-LABEL-MIB                      -
SNMPv2-MIB                               1.3.6.1.2.1
IF-MIB                                   1.3.6.1.2.1.31
IP-MIB                                   1.3.6.1.2.1.48
TCP-MIB                                  1.3.6.1.2.1.49
UDP-MIB                                  1.3.6.1.2.1.50
RFC1213-MIB                              -
EtherLike-MIB                            1.3.6.1.2.1.35
SNMP-FRAMEWORK-MIB                       1.3.6.1.6.3.10
RADIUS-AUTH-CLIENT-MIB                   1.3.6.1.2.1.67.1.2
SNMP-MPD-MIB                             1.3.6.1.6.3.11
RMON-MIB                                 1.3.6.1.2.1.16
--More--
```

show snmp supported-traps

Display the list of SNMP traps supported by the platform.

Syntax

```
show snmp supported-traps
```

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the C9010, FN-IOM, MIOA, MXL, S3048–ON, S3100, S4048–ON, S4048T-ON, S5048F-ON, S6000, S6000–ON, S6010–ON, S6100–ON and Z9100–ON.

Example

```
DellEMC#show snmp supported-traps
TRAP                                          OID
-------------------------------------------------------------------
COLDSTART                                     1.3.6.1.6.3.1.1.5.1
WARMSTART                                     1.3.6.1.6.3.1.1.5.2
LINKDOWN                                      1.3.6.1.6.3.1.1.5.3
LINKUP                                        1.3.6.1.6.3.1.1.5.4
Authenticationfailure                         1.3.6.1.6.3.1.1.5.5
dellNetIfAlarmHighBer                         1.3.6.1.4.1.6027.3.11.1.4.1.1
dellNetIfAlarmHighBerClr                      1.3.6.1.4.1.6027.3.11.1.4.1.2
dellNetSysAlarmCardDown                       1.3.6.1.4.1.6027.3.26.1.5.1.1
dellNetSysAlarmCardUp                         1.3.6.1.4.1.6027.3.26.1.5.1.2
dellNetSysAlarmCardOffline                    1.3.6.1.4.1.6027.3.26.1.5.1.3
dellNetSysAlarmCardMismatch                   1.3.6.1.4.1.6027.3.26.1.5.1.4
dellNetSysAlarmRpmUp                          1.3.6.1.4.1.6027.3.26.1.5.1.5
dellNetSysAlarmRpmDown                        1.3.6.1.4.1.6027.3.26.1.5.1.6
dellNetSysAlarmPowersupplyDown                1.3.6.1.4.1.6027.3.26.1.5.1.7
dellNetSysAlarmMinorTemperatureHigh           1.3.6.1.4.1.6027.3.26.1.5.1.8
dellNetSysAlarmMajorTemperatureHigh           1.3.6.1.4.1.6027.3.26.1.5.1.9
dellNetSysAlarmFanTrayDown                    1.3.6.1.4.1.6027.3.26.1.5.1.10
dellNetSysAlarmPowersupplyClear               1.3.6.1.4.1.6027.3.26.1.5.1.11
```

```
dellNetSysAlarmMinorTemperatureClear     1.3.6.1.4.1.6027.3.26.1.5.1.12
dellNetSysAlarmMajorTemperatureClear     1.3.6.1.4.1.6027.3.26.1.5.1.13
dellNetSysAlarmFanTrayClear              1.3.6.1.4.1.6027.3.26.1.5.1.14
--More--
```

show snmp user

Display the information configured on each SNMP user name.

C9000 Series

Syntax `show snmp user`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
Dell#show snmp user
  User name: v1v2creadu
  Engine ID: 0000178B02000001E80214A8
  storage-type: nonvolatile     active
  Authentication Protocol: None
  Privacy Protocol: None

Dell#
```

snmp context

Enables you to map a bgp vrf instance within a SNMP context through community mapping, in SNMPv2c and SNMPv3.

Syntax `[no] snmp context [context name]`

Parameters

context name	Enter a unique name for the context.

Defaults None

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13(0.0)	Introduced on all DNOS platforms.

Usage Information This command is used for mapping SNMP context to a VRF instance within a community, in SNMPv2c and SNMPv3. The no version of this command turns off this feature.

snmp ifmib ifalias long

Display the entire description string through the Interface MIB, which would be truncated otherwise to 63 characters.

C9000 Series

Syntax

```
snmp ifmib ifalias long
```

Defaults Interface description truncated beyond 63 characters.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
!----command run on host connected to switch:------!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2. This
is a
port connected to
IF-MIB::ifAlias.134792448 = STRING:
```

```
!----command run on Force10 switch:-----------!
Dell#snmp ifmib ifalias long

!----command run on server connected to switch:------!
> snmpwalk -c public 10.10.10.130 .1.3.6.1.2.1.31 | grep -i alias | more
IF-MIB::ifAlias.134530304 = STRING: This is a port connected to Router2. This
is a
port connected to Router2. This is a port connected to Router2. This is a port
connected to Router2. This is a port connected to Router2.
IF-MIB::ifAlias.134792448 = STRING:
```

snmp mib community-map

Associate an SNMP community context (string) with an SNMP context community-map

C9000 Series

Syntax

```
snmp mib community-map name context name
```

Defaults

Community name is limited to 20 characters.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Example

```
Dell(conf)#snmp mib ?
community-map           Map a SNMP community String with a SNMP context
Dell(conf)#snmp mib community-map ?
WORD                    Name of the Community(Max 20 chars)
Dell(conf)#snmp mib community-map rise1 ?
context                 Snmp Context
Dell(conf)#snmp mib community-map rise1 context ?
WORD                    SNMP Context Name(Max 32 chars)
```

snmp-server contact

Configure contact information for troubleshooting this SNMP node.

C9000 Series

Syntax

```
snmp-server contact text
```

To delete the SNMP server contact information, use the `no snmp-server contact` command.

Parameters

text	Enter an alphanumeric text string, up to 55 characters long.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

snmp-server context

Configure a new context string for SNMP (SNMPv3) server.

C9000 Series

Syntax `snmp-server context {line}`

To remove a user from the SNMP group, use the `no snmp-server context {line}` command.

Parameters

line	Enter the context string (max 32 characters), on the host that connects to the agent.

Defaults NONE.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Usage Information

Example

```
Dell(conf)#snmp-server context line
```

Related Commands show snmp user — displays the information configured on each SNMP user name.

snmp-server community

Configure a new community string access for SNMPv1 v2 and v3.

C9000 Series

Syntax

`snmp-server community` *community-name* `{ro | rw} [ipv6` *ipv6-access-list-name* `[ipv6` *ipv6-access-list-name* `|` *access-list-name* `| security-name` *name*`] | security-name` *name* `[ipv6` *ipv6-access-list-name* `|` *access-list-name* `| security-name` *name*`] |` *access-list-name* `[ipv6` *ipv6-access-list-name* `|` *access-list-name* `| security-name` *name*`]]]`

To remove access to a community, use the `no snmp-server community` *community-string* `{ro | rw} [security-name` *name* `[`*access-list-name* `| ipv6` *access-list-name* `|` *access-list-name* `ipv6` *access-list-name*`]]` command.

Parameters

community-name	Enter a text string (up to 20 characters long) to act as a password for SNMP.
ro	Enter the keyword `ro` to specify read-only permission.
rw	Enter the keyword `rw` to specify read-write permission.
ipv6 ***access-list-name***	(Optional) Enter the keyword `ipv6` then an IPv6 ACL name (a string up to 16 characters long).
security-name ***name***	(Optional) Enter the keywords `security-name` then the security name as defined by the community MIB.
access-list-name	(Optional) Enter a standard IPv4 access list name (a string up to 16 characters long).

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

The following example configures a community named *public* that is mapped to the security named *guestuser* with Read Only (`ro`) permissions.

The `security-name` parameter maps the community string to an SNMPv3 user/security name as defined by the community MIB.

If a community string is configured without a `security-name` (for example, `snmp-server community public ro`), the community is mapped to a default security-name/group:

- `v1v2creadu / v1v2creadg` — maps to a community with `ro` (read-only) permissions.
- `v1v2cwriteu/ v1v2cwriteg` — maps to a community with `rw` (read-write) permissions.

The `community-name` parameter indexes this command.

If you do not configure the `snmp-server community` command, you cannot query SNMP data. Only Standard IPv4 ACL and IPv6 ACL is supported in the optional `access-list-name`.

The command options `ipv6`, `security-name`, and `access-list-name` are recursive. In other words, each option can, in turn, accept any of the three options as a sub-option, and each of those sub-options can accept any of the three sub-options as a sub-option, and so forth. The second Example shows the creation of a standard IPv4 ACL called *snmp-ro-acl* and then assigning it to the SNMP community *guest*.

NOTE: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP; TCP and ICMP rules are not valid for SNMP. In IPv6 ACLs, port rules are not valid for SNMP.

Example

```
Dell#config
Dell(conf)# snmp-server community public ro
Dell(conf)# snmp-server community public ro security-name guestuser
Dell(conf)#
```

Example

```
Dell(conf)# ip access-list standard snmp-ro-acl
Dell(config-std-nacl)#seq 5 permit host 10.10.10.224
Dell(config-std-nacl)#seq 10 deny any count
!

Dell(conf)#snmp-server community guest ro snmp-ro-acl
Dell(conf)#
```

Related Commands

ip access-list standard — names (or selects) a standard access list to filter based on IP address.

ipv6 access-list — configures an access list based on IPv6 addresses or protocols.

show running-config — displays the current SNMP configuration and defaults.

snmp-server enable traps

Enable SNMP traps.

C9000 Series

Syntax

```
snmp-server enable traps [notification-type] [notification-option]
```

To disable traps, use the `no snmp-server enable traps [notification-type] [notification-option]` command.

Parameters

notification-type Enter the type of notification from the following list:

- `bgp` — Enable notification of changes in the BGP process.
- `config` — Enable notification of changes to startup or running configuration.
- `dot1br`— Enable notification of changes to DOT1BR.
- `ecfm` — Enable notification of changes to ECFM.
- `ecmp` — Enable notification of traffic imbalance in ECMP or a link bundle.
- `entity` —Enable notification of Entity Management Information Base (MIB) changes.
- `envmon` — Enable notification when an environmental threshold is exceeded.
- `ets` — Enable notification of ETS changes.
- `fips` — Enable notification of a FIP Snooping state changes.
- `hg-lbm` — Enable notification of hiGig link-bundle state changes.
- `isis` — Enable notification of IS-IS adjacency state changes.
- `pfc` — Enable notification of changes to PFC.
- `lacp` — Enable notification of LACP state changes.
- `snmp` — Enable SNMP notifications defined in RFC 1157.
- `stp` — Enable notification of a state change in the spanning tree protocol (RFC 1493).
- `vlt` — Enable notification of VLT state changes.
- `vrrp` —Enable notification of a state change in a VRRP group.
- `xstp` — Enable notification of a state change in MSTP (802.1s), RSTP (802.1w), and PVST+.

notification-option For the `envmon` notification-type, enter one of the following optional parameters:

- `cam-utilization`
- `fan`
- `supply`
- `temperature`

For the `snmp` notification-type, enter one of the following optional parameters:

- `authentication`
- `coldstart`
- `linkdown`
- `linkup`

Defaults Not enabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for copy-config and ecmp traps.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Added support for VRRP traps.
7.6.1.0	Added support for STP and xSTP traps. Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

The system supports up to 16 SNMP trap receivers.

For the `cam-utilization` notification option, the system generates syslogs and SNMP traps when the L3 host table or route table utilization goes above the threshold.

If you do not configure this command, no traps controlled by this command are sent. If you do not specify a `notification-type` and `notification-option`, all traps are enabled.

Related Commands

snmp-server community — enables SNMP and sets the community string.

snmp-server host — configures an SNMP trap receiver.

snmp-server engineID

Configure the name for both the local and remote SNMP engines on the router.

C9000 Series

Syntax

```
snmp-server engineID [local engineID] [remote ip-address vrf management udp-port port-number engineID]
```

To return to the default, use the `no snmp-server engineID [local engineID] [remote ip-address vrf management udp-port port-number engineID]` command.

Parameters

local *engineID*

Enter the keyword `local` followed by the engine ID number that identifies the copy of the SNMP on the local device.

Format (as specified in RFC 3411): 12 octets.

- The first four octets are set to the private enterprise number.
- The remaining eight octets are the MAC address of the chassis.

remote *ip-address*

Enter the keyword `remote` followed by the IP address that identifies the copy of the SNMP on the remote device.

vrf *management*	(OPTIONAL) Enter the keyword `vrf`followed by the keyword `management` to specify that management vrf will be used to reach the remote host.
udp-port *port-number engineID*	Enter the keywords `udp-port` followed by the user datagram protocol (User Datagram Protocol) port number on the remote device. The range is from 0 to 65535. The default is **162**.

Defaults As above.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information Changing the value of the SNMP Engine ID has important side effects. A user's password (entered on the command line) is converted to a message digest algorithm (MD5) or secure hash algorithm (SHA) security digest. This digest is based on both the password and the local Engine ID. The command line password is then destroyed, as required by RFC 2274. Because of this deletion, if the local value of the Engine ID changes, the security digests of SNMPv3 users is invalid and the users will have to be reconfigured.

For the remote Engine ID, the host IP and UDP port are the indexes to the command that are matched to either overwrite or remove the configuration.

Related Commands show snmp engineID — displays the SNMP engine and all the remote engines that are configured on the router.

show running-config snmp — displays the SNMP running configuration.

snmp-server group

Configure a new SNMP group or a table that maps SNMP users to SNMP views.

C9000 Series

Syntax

```
snmp-server group [group_name {1 | 2c | 3 {auth | noauth | priv}}] [read name]
[write name] [notify name] [access access-list-name | ipv6 access-list-name |
access-list-name ipv6 access-list-name]]
```

To remove a specified group, use the `no snmp-server group [group_name {v1 | v2c | v3 {auth | noauth | priv}}] [read name] [write name] [notify name] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]` command.

Parameters

group_name	Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults): • `v1v2creadg` — maps to a community/security-name with `ro` permissions. • `1v2cwriteg` — maps to a community/security-name `rw` permissions.
1 | 2c | 3	(OPTIONAL) Enter the security model version number (`1`, `2c`, or `3`): • `1` is the least secure version. • `3` is the most secure of the security modes. • `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. The default is **1**.
auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword `noauth` to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword `priv` to specify both authentication and then scrambling of the packet.
read *name*	(OPTIONAL) Enter the keyword `read` then a name (a string of up to 20 characters long) as the read view name. The default is **GlobalView** and is assumed to be every object belonging to the internet (1.3.6.1) OID space.
write *name*	(OPTIONAL) Enter the keyword `write` then a name (a string of up to 20 characters long) as the write view name.
notify *name*	(OPTIONAL) Enter the keyword `notify` then a name (a string of up to 20 characters long) as the notify view name.
access *access-list-name*	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).
ipv6 *access-list-name*	(Optional) Enter the keyword `ipv6` then the IPv6 access list name (a string up to 16 characters long).
access-list-name ipv6 *access-list-name*	(Optional) Enter both an IPv4 and IPv6 access list name.

Defaults As above.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.2	Added support for the `access` parameter.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

The following Example specifies the group named *harig* as a version 3 user requiring both authentication and encryption and read access limited to the read named *rview*.

NOTE: The number of configurable groups is limited to 16 groups.

Example

```
Dell#conf
Dell(conf)# snmp-server group harig 3 priv read rview
Dell#
```

Related Commands

show snmp group — displays the group name, security model, view status, and storage type of each group.

show running-config — displays the SNMP running configuration.

snmp-server host

Configure the recipient of an SNMP trap operation.

C9000 Series

Syntax

`snmp-server host ip-address | ipv6-address | hostname [vrf management traps | informs] [version 1 | 2c | 3] [auth | no auth | priv] [community-string] [udp-port port-number] [notification-type]`

To remove the SNMP host, use the no snmp-server host ip-address | ipv6-address | *hostname* [vrf *management* traps | informs] [version 1 | 2c | 3] [auth | noauth | priv] [community-string] [udp-port number] [notification-type] command.

Parameters

ip-address	Enter the keyword `host` followed by the IP address of the host (Configurable hosts are limited to 16).
ipv6-address	Enter the keyword host then the IPv6 address of the host in the x:x:x:x::x format. **NOTE: The :: notation specifies successive hexadecimal fields of zero.**
hostname	Enter the keyword `host` followed by the name of a host already configured and recognized by the switch.

vrf *management*	Enter the keyword `vrf` followed by the keyword management to specify that management vrf will be used to send traps and informs.
traps	(OPTIONAL) Enter the keyword `traps` to send trap notifications to the specified host. The default is **traps**.
informs	(OPTIONAL) Enter the keyword `informs` to send inform notifications to the specified host. The default is **traps**.
version 1 | 2c | 3	(OPTIONAL) Enter the keyword version to specify the security model then the security model version number `1`, `2c`, or `3`: • Version `1` is the least secure version. • Version `3` is the most secure of the security modes. • Version `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. The default is version **1**.
auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword `noauth` to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword `priv` to specify both authentication and then scrambling of the packet.
community-string	Enter a text string (up to 20 characters long) as the name of the SNMP community. **NOTE: For version 1 and version 2c security models, this string represents the name of the SNMP community. The string can be set using this command; however, Dell Networking recommends setting the community string using the `snmp-server community` command before executing this command. For version 3 security model, this string is the USM user security name.**
udp-port *port-number*	(OPTIONAL) Enter the keywords `udp-port` followed by the port number of the remote host to use. The range is from 0 to 65535. The default is **162**.
notification-type	(OPTIONAL) Enter one of the following keywords for the type of trap to be sent to the host: • `bgp` — BGP state change. • `config` — copy—configuration traps. • `ecmp` — ecmp and link bundling traffic imbalance traps. • `entity` — Entity state change. • `envmon` — Environment monitor trap. • `hg-lbm` — HiGig link bundle state change. • `isis` — ISIS adjacency state change. • `lacp` — LACP state change. • `snmp` — SNMP notification (RFC 1157). • `stp` — Spanning tree protocol notification (RFC 1493). • `vlt` — VLT state change. • `vrrp` — State change in a VRRP group. • `xstp` — State change in MSTP (802.1s), RSTP (802.1w), and PVST+.

The default is all trap types, which are sent to the host.

Defaults As above.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.1(0.0)	Added support for config and ecmp traps.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Added support for VRRP traps.
7.6.1.0	Added support for STP and xSTP notification types. Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information In order to configure the router to send SNMP notifications, enter at least `one snmp-server host` command. If you enter the command with no keywords, all trap types are enabled for the host. If you do not enter an `snmp-server host` command, no notifications are sent.

In order to enable multiple hosts, issue a separate `snmp-server host` command for each host. You can specify multiple notification types in the command for each host.

When multiple `snmp-server host` commands are given for the same host and type of notification (trap or inform), each succeeding command overwrites the previous command. Only the last `snmp-server host` command will be in effect. For example, if you enter an `snmp-server host inform` command for a host and then enter another `snmp-server host inform` command for the same host, the second command replaces the first command.

The `snmp-server host` command is used with the `snmp-server enable` command. Use the `snmp-server enable` command to specify which SNMP notifications are sent globally. For a host to receive most notifications, at least one `snmp-server enable` command and the `snmp-server host` command for that host must be enabled.

NOTE: For v1 / v2c trap configuration, if the community-string is not defined using the `snmp-server community` command prior to using this command, the default form of the `snmp-server community` command automatically is configured with the community-name the same as specified in the `snmp-server host` command.

Configuring Informs

To send an inform, use the following steps:

1 Configure a remote engine ID.

2 Configure a remote user.
3 Configure a group for this user with access rights.
4 Enable traps.
5 Configure a host to receive informs.

Related Commands snmp-server enable traps — enables SNMP traps.

snmp-server community — configures a new community SNMPv1 or SNMPv2c.

snmp-server location

Configure the location of the SNMP server.

C9000 Series

Syntax `snmp-server location text`

To delete the SNMP location, use the `no snmp-server location` command.

Parameters

text	Enter an alpha-numeric text string, up to 55 characters long.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example

```
Dell(conf)#snmp-server location MAA_LAB
Dell(conf)#do show running-config snmp
!
snmp-server community public ro
snmp-server location MAA_LAB
```

Related Commands show running-config snmp — displays the SNMP running configuration.

snmp-server packetsize

Set the largest SNMP packet size permitted. Wen the SNMP server is receiving a request or generating a reply, use the `snmp-server packetsize global configuration` command.

C9000 Series

Syntax `snmp-server packetsize byte-count`

Parameters

byte-count	Enter one of the following values 8, 16, 24 or 32. Packet sizes are 8000 bytes, 16000 bytes, 32000 bytes, and 64000 bytes.

Defaults **8**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

snmp-server trap-source

Configure a specific interface as the source for SNMP traffic.

C9000 Series

Syntax `snmp-server trap-source interface`

To disable sending traps out a specific interface, use the `no snmp trap-source` command.

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults The IP address assigned to the management interface is the default.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information To enable this `snmp-server trap-source` command, configure an IP address on the interface and enable the interface configured as an SNMP trap source.

Related Commands snmp-server community — sets the community string.

snmp-server user

Configure a new user to an SNMP group.

C9000 Series

Syntax

```
snmp-server user name {group_name remote ip-address udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv {des56 | aes128} priv password] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]
```

To remove a user from the SNMP group, use the `no snmp-server user name {group_name remote ip-address udp-port port-number} [1 | 2c | 3] [encrypted] [auth {md5 | sha} auth-password] [priv {des56 | aes128} priv password] [access access-list-name | ipv6 access-list-name | access-list-name ipv6 access-list-name]` command.

Parameters

name Enter the name of the user (not to exceed 20 characters), on the host that connects to the agent.

group_name	Enter a text string (up to 20 characters long) as the name of the group. The following groups are created for mapping to read/write community/security-names (defaults): • `v1v2creadu` — maps to a community with `ro` permissions. • `1v2cwriteu` — maps to a community `rw` permissions.
remote *ip-address*	Enter the keywords `udp-port` then the user datagram protocol (UDP) port number on the remote device. The range is from 0 to 65535. The default is **162**.
udp-port *port-number*	Enter the keywords `udp-port` then the UDP (User Datagram Protocol) port number on the remote device. The range is from 0 to 65535. The default is **162**.
1 | 2c | 3	(OPTIONAL) Enter the security model version number (`1`, `2c`, or `3`): • `1` is the least secure version. • `3` is the most secure of the security modes. • `2c` allows transmission of informs and counter 64, which allows for integers twice the width of what is normally allowed. The default is **1**.
encrypted	(OPTIONAL) Enter the keyword `encrypted` to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).
auth	(OPTIONAL) Enter the keyword `auth` to specify authentication of a packet without encryption.
md5 | sha	(OPTIONAL) Enter the keyword `md5` or `sha` to designate the authentication level. • `md5` — Message Digest Algorithm • `sha` — Secure Hash Algorithm
auth-password	(OPTIONAL) Enter a text string (up to 20 characters long) password that enables the agent to receive packets from the host. Minimum: eight characters long.
priv	(OPTIONAL) Enter the keywords `priv` to initiate a privacy authentication level setting.
des56 | aes128	(OPTIONAL) Enter the keyword `des56` or `aes128` to specify the encryption mode. • `aes128` — Use 128 bit AES algorithm in CFB mode for encryption. • `des56` — Use 56 bit DES algorithm in CBC mode for encryption.
priv password	(OPTIONAL) Enter a text string (up to 20 characters long) password that enables the host to encrypt the contents of the message it sends to the agent. Minimum: eight characters long.
access *access-list-name*	(Optional) Enter the standard IPv4 access list name (a string up to 16 characters long).
ipv6 *access-list-name*	(Optional) Enter the keyword `ipv6` then the IPv6 access list name (a string up to 16 characters long).
access-list-name ipv6 access-list-name	(Optional) Enter both an IPv4 and IPv6 access list name.

Defaults As above.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6.(0.0)	Added aes 128 encryption algorithm parameter.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information

NOTE: For IPv6 ACLs, only IPv6 and UDP types are valid for SNMP. TCP and ICMP rules are not valid for SNMP. In IPv6 ACLs port rules are not valid for SNMP.

No default values exist for authentication or privacy algorithms and no default password exists. If you forget a password, you cannot recover it; the user must be reconfigured. You can specify either a plain-text password or an encrypted cypher-text password. In either case, the password is stored in the configuration in an encrypted form and displayed as encrypted in the `show running-config` command.

If you have an encrypted password, you can specify the encrypted string instead of the plain-text password. The following command is an Example of how to specify the command with an encrypted string.

NOTE: The number of configurable users is limited to 16.

Example

```
Dell# snmp-server user privuser v3group v3 encrypted auth md5
9fc53d9d908118b2804fe80e3ba8763d priv des56 d0452401a8c3ce42804fe80e3ba8763d
```

Usage Information The following command is an example of how to enter a plain-text password as the string `authpasswd` for user `authuser` of group `v3group`.

Example

```
Dell#conf
Dell(conf)# snmp-server user authuser v3group v3 auth md5 authpasswd
```

Usage Information The following command configures a remote user named *n3user* with a v3 security model and a security level of `authNOPriv`.

Example

```
Dell#conf
Dell(conf)# snmp-server user n3user ngroup remote 172.31.1.3 udp-port 5009 3
auth md5 authpasswd
```

Related Commands show snmp user — displays the information configured on each SNMP user name.

snmp-server view

Configure an SNMPv3 view.

C9000 Series

Syntax

`snmp-server view` *`view-name oid-tree`* `{included | excluded}`

To remove an SNMPv3 view, use the `no snmp-server view` *`view-name oid-tree`* `{included | excluded}` command.

Parameters

view-name	Enter the name of the view (not to exceed 20 characters).
oid-tree	Enter the OID sub tree for the view (not to exceed 20 characters).
included	(OPTIONAL) Enter the keyword `included` to include the MIB family in the view.
excluded	(OPTIONAL) Enter the keyword `excluded` to exclude the MIB family in the view.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information The `oid-tree` variable is a full sub-tree starting from 1.3.6 and cannot specify the name of a sub-tree or a MIB. The following Example configures a view named *rview* that allows access to all objects under 1.3.6.1.

Example

```
Dell# conf
Dell#(conf) snmp-server view rview 1.3.6.1 included
```

Related Commands show running-config snmp — displays the SNMP running configuration.

snmp-server vrf

Configures an SNMP agent to bind to a specific VRF.

C9000 Series

Syntax

`snmp-server vrf vrf-name`

To undo the SNMP agent configuration, use the `no snmp-server vrf vrf-name` command.

Parameters

vrf vrf-name	Enter the keyword `vrf` and then the name of the VRF to associate an SNMP agent with that VRF.

Defaults

default

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S-Series and Z9000.

Usage Information

Use this command to bind an SNMP agent to a VRF. The SNMP agent processes the requests from the interfaces that belong to the specified VRF. If no VRF is specified, then the default VRF is used.

Related Commands

show snmp user — displays the information configured on each SNMP user name.

snmp trap link-status

Enable the interface to send SNMP link traps, which indicate whether the interface is up or down.

C9000 Series

Syntax

`snmp trap link-status`

To disable sending link trap messages, use the `no snmp trap link-status` command.

Defaults

Enabled.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

If the interface is expected to flap during normal usage, you could disable this command.

Syslog Commands

The following commands allow you to configure logging functions on all Dell Networking switches.

clear logging

Clear the messages in the logging buffer.

C9000 Series

Syntax

```
clear logging
```

From a **PE console**, use `clear logging` to clear the messages in the logging buffer.

Defaults

none

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information To clear the messages in the logging buffer from a port extender (PE) console, use the `clear logging` command.

Related Commands show logging — displays logging settings and system messages in the internal buffer.

clear logging auditlog

Clears audit log.

C9000 Series

Syntax `clear logging auditlog`

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.

Example

```
Dell(conf)#clear logging auditlog
```

Related Commands show logging auditlog — displays audit log

default logging buffered

Return to the default setting for messages logged to the internal buffer.

C9000 Series

Syntax `default logging buffered`

Defaults **size = 40960; level = 7 or debugging**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands logging buffered — sets the logging buffered parameters.

default logging console

Return the default settings for messages logged to the console.

C9000 Series

Syntax `default logging console`

Defaults **level = 7 or debugging**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands logging console — sets the logging console parameters.

default logging monitor

Return to the default settings for messages logged to the terminal.

C9000 Series

Syntax	`default logging monitor`
Defaults	**level = 7 or debugging**
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands	logging monitor — sets the logging monitor parameters. terminal monitor — sends system messages to the terminal/monitor.

default logging trap

Return to the default settings for logging messages to the Syslog servers.

C9000 Series

Syntax	`default logging trap`
Defaults	**level = 6 or informational**
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*. The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands logging trap — limit messages logged to the Syslog servers based on severity.

logging

Configure an IP address or host name of a Syslog server where logging messages are sent. Multiple logging servers of both IPv4 and/or IPv6 can be configured.

C9000 Series

Syntax

`logging {`*`ip-address`* `|` *`ipv6-address`* `|` *`hostname`*`} {`*`vrf management`*`}{udp {`*`port`*`}} | {tcp {port}}`

To disable logging, use the `no logging {`*`ip-address`* `|` *`ipv6-address`* `|` *`hostname`*`} {`*`vrf management`*`} | {udp {`*`port`*`}} | {tcp {port}}` command.

Parameters

ip-address	Enter the IPv4 address in dotted decimal format.
ipv6-address	Enter the IPv6 address in the x:x:x:x::X format. **NOTE: The :: notation specifies successive hexadecimal fields of zeros.**
hostname	Enter the name of a host already configured and recognized by the switch.
management	Management VRF name to be used to reach host.
udp	Enter the keyword `udp` to enable transmission of log message over UDP followed by port number. The default port is 514
tcp	Enter the keyword `tcp` to enable transmission of log message over TCP followed by port number.

Defaults Disabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.x.x.x	Introduced on the C9000.

Version	Description
9.5(0.1)	Added **udp** and **tcp** keywords for the Z9500.
9.5(0.0)	Added **udp** and **tcp** keywords for the S4810, S4820T, S6000, Z9000, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.4.1.0	Added support for IPv6.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information Multiple logging servers of both IPv4 and/or IPv6 can be configured.

Related Commands logging on — enables the logging asynchronously to logging buffer, console, Syslog server, and terminal lines.

logging trap — enables logging to the Syslog server based on severity.

logging buffered

Enable logging and specify which messages are logged to an internal buffer. By default, all messages are logged to the internal buffer.

C9000 Series

Syntax `logging buffered [level] [size]`

To return to the default values, use the `default logging buffered` command.

To disable logging stored to an internal buffer, use the `no logging buffered` command.

Parameters

level	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following equivalent words: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.
size	(OPTIONAL) Indicate the size, in bytes, of the logging buffer. The number of messages buffered depends on the size of each message. The range is from 40960 to 524288. The default is **40960 bytes**.

Defaults level = **7**; size = **40960 bytes**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information When you decrease the buffer size, all messages stored in the buffer are lost. Increasing the buffer size does not affect messages stored in the buffer.

Related Commands clear logging — clears the logging buffer.

default logging buffered — returns the logging buffered parameters to the default setting.

show logging — displays the logging setting and system messages in the internal buffer.

logging console

Specify which messages are logged to the console.

C9000 Series

Syntax `logging console [level]`

To return to the default values, use the `default logging console` command.

To disable logging to the console, use the `no logging console` command.

Parameters

level	(OPTIONAL) Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.

Defaults level = **7**; size = **debugging**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands

clear logging — clears the logging buffer.

default logging console — returns the logging console parameters to the default setting.

show logging — displays the logging setting and system messages in the internal buffer.

logging coredump stack-unit

Enable coredump on a stack.

C9000 Series

Syntax

```
logging coredump stack-unit {0-5 | all}
```

Parameters

stack-unit 0–5	Enter the stack-unit id.
all	Enable coredump on all stack-unit.

Defaults

Enabled by default on customer builds.

Command Modes

CONFIGURATION

Command History

Version	Description
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Usage Information

The Kernel core dump can be large and may take up to 5 to 30 minutes to upload. Dell Networking OS does not overwrite application core dumps so you should delete them as necessary to conserve space on the flash; if the flash is out of memory, the coredump is aborted. On the S-Series, if the FTP server is not reachable, the application coredump is aborted. Dell Networking OS completes the coredump process and wait until the upload is complete before rebooting the system.

logging extended

Logs security and audit events to a system log server.

C9000 Series

Syntax `logging extended`

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.

Usage Information This command is available with or without RBAC enabled. When RBAC is enabled you can restrict access to audit and security logs based on the CLI sessions' user roles. If extended logging is disabled, you can only view system events, regardless of RBAC user role.

When you enabled RBAC and extended logging:

- Only the system administrator role can execute this command.
- The system administrator and system security administrator roles can view security events and system events.
- The system administrator role can view audit, security, and system events.
- The network administrator and network operator roles can view system events.

Examples

```
Dell(conf)#logging extended
```

Related Commands

- clear logging auditlog — clears audit log
- show logging auditlog — displays audit log.

logging facility

Configure the Syslog facility used for error messages sent to Syslog servers.

C9000 Series

Syntax `logging facility [facility-type]`

To return to the default values, use the `no logging facility` command.

Parameters

facility-type (OPTIONAL) Enter one of the following parameters:

- `auth` (authorization system)
- `cron` (Cron/at facility)
- `deamon` (system deamons)
- `kern` (kernel)
- `local0` (local use)
- `local1` (local use)
- `local2` (local use)
- `local3` (local use)
- `local4` (local use)
- `local5` (local use)
- `local6` (local use)
- `local7` (local use)
- `lpr` (line printer system)
- `mail` (mail system)
- `news` (USENET news)
- `sys9` (system use)
- `sys10` (system use)
- `sys11` (system use)
- `sys12` (system use)
- `sys13` (system use)
- `sys14` (system use)
- `syslog` (Syslog process)
- `user` (user process)
- `uucp` (Unix to Unix copy process)

The default is **local7**.

Defaults **local7**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.

Related Commands logging — enables logging to a Syslog server.

logging on — enables logging.

logging history

Specify which messages are logged to the history table of the switch and the SNMP network management station (if configured).

C9000 Series

Syntax `logging history level`

To return to the default values, use the `no logging history` command.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following equivalent words: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **4** or **warnings**.

Defaults **warnings or 4**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information When you configure the `snmp-server trap-source` command, the system messages logged to the history table are also sent to the SNMP network management station.

Related Commands show logging — displays information logged to the history buffer.

logging history size

Specify the number of messages stored in the logging history table.

C9000 Series

Syntax

`logging history size size`

To return to the default values, use the `no logging history size` command.

Parameters

size	Indicate a value as the number of messages to be stored. The range is from 0 to 500. The default is **1 message**.

Defaults

1 message

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

When the number of messages reach the limit you set with the `logging history size` command, older messages are deleted as newer ones are added to the table.

Related Commands

show logging — displays information logged to the history buffer.

logging monitor

Specify which messages are logged to Telnet applications.

C9000 Series

Syntax

`logging monitor [level]`

To disable logging to terminal connections, use the `no logging monitor` command.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **7** or **debugging**.

Defaults **7** or **debugging**

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands default logging monitor — returns the logging monitor parameters to the default setting.

logging on

Specify that debug or error messages are asynchronously logged to multiple destinations, such as the logging buffer, Syslog server, or terminal lines.

C9000 Series

Syntax `logging on`

To disable logging to logging buffer, Syslog server and terminal lines, use the `no logging on` command.

Defaults Enabled.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information When you use the `no logging on` command, messages are logged only to the console.

Related Commands logging — enables logging to the Syslog server.

logging buffered — sets the logging buffered parameters.

logging console — sets the logging console parameters.

logging monitor — sets the logging parameters for the terminal connections.

logging source-interface

Specify that the IP address of an interface is the source IP address of Syslog packets sent to the Syslog server.

C9000 Series

Syntax `logging source-interface` *interface*

To disable this command and return to the default setting, use the `no logging source-interface` command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For Loopback interfaces, enter the keyword `loopback` then a number from zero (0) to 16383.
- For the management interface on the RPM, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 0 to 1 and the port range is 0.
- For a Port Channel interface, enter the keywords `port-channel` then a number. Tthe range is from 1 to 4096.
- For a ten-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information Syslog messages contain the IP address of the interface used to egress the router. By configuring the `logging source-interface` command, the Syslog packets contain the IP address of the interface configured.

Related Commands logging — enables logging to the Syslog server.

logging synchronous

Synchronize unsolicited messages and output.

C9000 Series

Syntax `logging synchronous [level level | all] [limit number-of-buffers]`

To disable message synchronization, use the `no logging synchronous [level level | all] [limit number-of-buffers]` command.

Parameters

all	Enter the keyword `all` to ensure that all levels are printed asynchronously.
level *level*	Enter the keyword `level` then a number as the severity level. A high number indicates a low severity level and vice versa. The range is from 0 to 7. The default is **2**.
all	Enter the keyword `all` to turn off all.
limit *number-of-buffers*	Enter the keyword `limit` then the number of buffers to be queued for the terminal after which new messages are dropped. The range is from 20 to 300. The default is **20**.

Defaults Disabled. If enabled without the `level` or `number-of-buffers` options specified, level = **2** and number-of-buffers = **20** are the defaults.

Command Modes LINE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Usage Information

When you enable `logging synchronous`, unsolicited messages appear between software prompts and outputs. Only the messages with a severity at or below the set level are sent to the console.

If the message queue limit is reached on a terminal line and messages are discarded, a system message appears on that terminal line. Messages may continue to appear on other terminal lines.

Related Commands

logging on — enables logging.

logging trap

Specify which messages are logged to the Syslog server based the message severity.

C9000 Series

Syntax

`logging trap [level]`

To return to the default values, use the `default logging trap` command.

To disable logging, use the `no logging trap` command.

Parameters

level	Indicate a value from 0 to 7 or enter one of the following parameters: `emergencies`, `alerts`, `critical`, `errors`, `warnings`, `notifications`, `informational`, or `debugging`. The default is **6** or **informational**.

Defaults

6 or **informational**

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series, S55.

Version	Description
7.5.1.0	Introduced on the C-Series.

Usage Information To block a type of message parameter, set the logging trap level to a lower number. For example, to block severity messages at level 6, set the level to 5.

Related Commands logging — enables the logging to another device.

logging on — enables logging.

logging version

Displays syslog messages in a RFC 3164 or RFC 5424 format.

C9000 Series

Syntax `logging version {0|1}`

Defaults 0

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.

Usage Information To display syslog messages in a RFC 3164 or RFC 5424 format, use the **log version** command in configuration mode. By default, the system log version is set to **0**.

The following describes the two supported log messages formats:

- 0 – Displays syslog messages format as described in RFC 3164, The BSD syslog Protocol
- 1 – Displays SYSLOG message format as described in RFC 5424, The Syslog Protocol

Example

```
Dell(conf)#logging version ?
<0-1> Select syslog version (default = 0)
Dell(conf)#logging version 1
```

show logging

Display the logging settings and system messages logged to the internal buffer of the switch.

C9000 Series

Syntax

`show logging [number | history [reverse][number] | reverse [number] | summary]`

From a **PE console**, use `show logging [number]`

Parameters

number	(OPTIONAL) Enter the number of messages displayed in the output. The range is from 1 to 65535.
history	(OPTIONAL) Enter the keyword `history` to view only information in the Syslog history table.
reverse	(OPTIONAL) Enter the keyword `reverse` to view the Syslog messages in FIFO (first in, first out) order.
summary	(OPTIONAL) Enter the keyword `summary` to view a table showing the number of messages per type and per slot. Slots *7* and *8* represent RPMs.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Example (Partial)

```
Dell#show logging

Syslog logging: enabled
    Console logging: level debugging
    Monitor logging: level debugging
    Buffer logging: level debugging, 97 Messages Logged, Size (40960 bytes)
    Trap logging: level informational
        Logging to 172.16.1.162
        Logging to 10.10.10.4
        Logging to 10.1.2.4
```

```
        Logging to 172.31.1.4
        Logging to 133.33.33.4
Feb 18 01:17:32: %SYSTEM:CP %SEC-5-LOGOUT: Exec session is terminated for user
admin on line vty0 ( 10.16.127.145 )
Feb 18 01:17:31: %SYSTEM:CP %IFMGR-5-ASTATE_DN: Changed interface Admin state
to down: Fo 2/0
Feb 18 01:17:24: %SYSTEM:CP %SEC-5-LOGIN_SUCCESS: Login successful for user
admin on line vty0 ( 10.16.127.145 )
Feb 18 01:17:23: %SYSTEM:CP %SEC-5-LOGOUT: Exec session is terminated for user
admin on line vty0 ( 10.16.127.145 )
Feb 18 01:17:03: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from vty0
( 10.16.127.145 )by admin
Feb 18 01:17:03: %SYSTEM:CP %IFMGR-5-ASTATE_UP: Changed interface Admin state
to up: Fo 2/0
Feb 18 01:16:57: %SYSTEM:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable
password authentication success on vty0 ( 10.16.127.145 )
Feb 18 01:16:57: %SYSTEM:CP %SEC-5-LOGIN_SUCCESS: Login successful for user
admin on line vty0 ( 10.16.127.145 )
Feb 18 00:46:18: %SYSTEM:CP %SEC-5-LOGOUT: Exec session is terminated for user
admin on line vty0 ( 10.16.127.145 )
Feb 18 00:46:17: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from vty0
( 10.16.127.145 )by admin
 - repeated 11 times
Feb 18 00:46:17: %SYSTEM:CP %IFMGR-5-ASTATE_DN: Changed interface Admin state
to down: Fo 2/0
Feb 18 00:45:46: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from vty0
( 10.16.127.145 )by admin
 - repeated 6 times
Feb 18 00:45:46: %SYSTEM:CP %IFMGR-5-ASTATE_UP: Changed interface Admin state
to up: Fo 2/0
Feb 18 00:45:40: %SYSTEM:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable
password authentication success on vty0 ( 10.16.127.145 )
Feb 18 00:45:40: %SYSTEM:CP %SEC-5-LOGIN_SUCCESS: Login successful for user
admin on line vty0 ( 10.16.127.145 )
Feb 18 00:43:10: %SYSTEM:CP %SEC-5-LOGOUT: Exec session is terminated for user
admin on line vty0 ( 10.16.127.145 )
Feb 18 00:43:10: %SYSTEM:CP %IFMGR-5-ASTATE_DN: Changed interface Admin state
to down: Fo 2/0
Feb 18 00:43:07: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from vty0
( 10.16.127.145 )by admin
 - repeated 6 times
Feb 18 00:42:44: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from vty0
( 10.16.127.145 )by admin
Feb 18 00:42:44: %SYSTEM:CP %IFMGR-5-ASTATE_UP: Changed interface Admin state
to up: Fo 2/0
Feb 18 00:42:38: %SYSTEM:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable
password authentication success on vty0 ( 10.16.127.145 )
Feb 18 00:42:38: %SYSTEM:CP %SEC-5-LOGIN_SUCCESS: Login successful for user
admin on line vty0 ( 10.16.127.145 )
Feb 18 00:39:38: %SYSTEM:CP %SYS-5-CONFIG_I: Configured from  console
--More--
```

Example (History)

```
Dell#show logging history

Syslog History Table: 1 maximum table entries,
saving level warnings or higher
 SNMP notifications not Enabled
Feb 18 01:16:57: %SYSTEM:CP %SEC-3-AUTHENTICATION_ENABLE_SUCCESS: Enable
password authentication success on vty0 ( 10.16.127.145 )
```

Example (PE Console)

```
Dell#show logging
Syslog logging: enabled
    Console logging: level debugging
    Monitor logging: level debugging
    Buffer logging: level debugging, 60 Messages Logged, Size (40960 bytes)
    Trap logging: level informational
Jul 30 16:34:27: %PE255-UNIT1-M:CP %CHMGR-4-TEMP_STATUS_CHANGE: Unit 3
temperature state changed to 1 (Current temperature 39C).
```

```
Jul 30 16:34:27: %PE-UNKN-C1048P:3 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 75 % of the full speed
Jul 30 16:34:26: %PE-UNKN-C1048P:3 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 60 % of the full speed
Jul 30 16:34:26: %PE255-UNIT1-M:CP %CHMGR-5-FANTRAY_INSERTED: Fan tray 0 of
Unit 3 is inserted
Jul 30 16:34:26: %PE-UNKN-C1048P:3 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 60 % of the full speed
Jul 30 16:34:26: %PE255-UNIT1-M:CP %CHMGR-0-PS_DOWN: Major alarm: Power supply
1 in unit 3 is down
Jul 30 16:34:26: %PE255-UNIT1-M:CP %CHMGR-5-PEM_INSERTED: Power entry module 1
of unit 3 is inserted
Jul 30 16:34:26: %PE255-UNIT1-M:CP %CHMGR-0-PS_UP: Power supply 0 in unit 3 is
up
Jul 30 16:34:26: %PE255-UNIT1-M:CP %CHMGR-5-PEM_INSERTED: Power entry module 0
of unit 3 is inserted
Jul 30 16:34:25: %PE-UNKN-C1048P:3 %IFAGT-5-INSERT_OPTICS_PLUS: Optics SFP+
inserted in slot 3 port 1
Jul 30 16:34:24: %PE255-UNIT1-M:CP %IFMGR-5-OSTATE_UP: Changed interface state
to up: Te 3/1
Jul 30 16:34:24: %PE-UNKN-C1048P:3 %IFAGT-5-STACK_PORT_LINK_UP: Changed stack
port state to up: 3/2
Jul 30 16:34:24: %PE-UNKN-C1048P:3 %IFAGT-5-STACK_PORT_LINK_UP: Changed stack
port state to up: 3/1
Jul 30 16:34:23: %PE255-UNIT1-M:CP %CHMGR-5-STACKUNIT_UP: stack-unit 3 is up
Jul 30 16:34:23: %PE255-UNIT1-M:CP %CHMGR-5-CHECKIN: Checkin from stack-unit 3
(type C1048P, 52 ports)
Jul 30 16:34:20: %PE255-UNIT1-M:CP %CHMGR-5-STACKUNIT_DETECTED: stack-unit 3
present
Jul 30 16:34:11: %PE255-C1048P:1 %IFAGT-5-STACK_PORT_LINK_UP: Changed stack
port state to up: 1/2
Jul 30 16:34:11: %PE255-C1048P:2 %IFAGT-5-STACK_PORT_LINK_UP: Changed stack
port state to up: 2/1
Jul 30 16:34:07: %PE255-UNIT2-S:CP %EVL-6-EVENT_LOGGING: Completed uploading
pre-recorded traps(send count:1, pending traps:0) to CB
Jul 30 16:34:07: %PE255-UNIT2-S:CP %EVL-6-EVENT_LOGGING: Start uploading pre-
recorded traps(count:1) to CB
Jul 30 16:34:05: %PE-UNKN-UNIT2-S:CP %RAM-5-STACKUNIT_STATE: Stack-unit 2 is
in Standby State.
Jul 30 16:33:17: %PE255-UNIT1-M:CP %IRC-6-IRC_COMMUP: Link to peer Stack-unit
is up
Jul 30 16:33:10: %PE255-UNIT1-M:CP %BRM-5-BRM_INVALID_PE_LLDP_TIMEOUT: LLDP PE
TLV timeout received info on interface TenGigabitEthernet 1/1 not matches
existing info in DB!
Jul 30 16:33:07: %PE255-UNIT1-M:CP %POLLMGR-2-ALT_STACKUNIT_STATE: Alternate
Stack-unit is present
Jul 30 16:33:03: %PE255-UNIT1-M:CP %SEC-5-LOGIN_SUCCESS: Login successful on
console
Jul 30 16:33:03: %PE255-UNIT1-M:CP %SEC-3-AUTHENTICATION_FAILURE:
Authentication failure on console for method "local" user ""
Jul 30 16:33:03: %PE255-UNIT1-M:CP %RAM-5-STACKUNIT_STATE: Stack-unit 1 is in
Active State.
Jul 30 16:33:02: %PE255-UNIT1-M:CP %RAM-5-HOT_FAILOVER: Stack-unit Failover
Completed.
Jul 30 16:33:02: %PE255-UNIT1-M:CP %CHMGR-2-SYSTEM_READY: System ready
Jul 30 16:33:01: %PE255-UNIT1-M:CP %CHMGR-2-SWITCH_MANAGEMENT: stack-unit 2
successfully switched to new Management stack-unit
Jul 30 16:32:59: %PE255-UNIT1-M:CP %IFMGR-1-DEL_PORT: Removed port:
Jul 30 16:32:59: %PE255-UNIT1-M:CP %IFMGR-5-OSTATE_DN: Changed interface state
to down: Te 3/1
Jul 30 16:32:59: %PE255-UNIT1-M:CP %CHMGR-2-STACKUNIT_DOWN: stack-unit 3 down
- card removed
Jul 30 16:32:59: %PE255-UNIT1-S:CP %POLLMGR-2-ALT_STACKUNIT_STATE: Alternate
Stack-unit is not present
Jul 30 16:32:58: %PE255-UNIT1-S:CP %RAM-6-ELECTION_ROLE: Stack-unit 1 is
transitioning to Management Stack-unit.
Jul 30 16:32:58: %PE255-UNIT1-S:CP %RAM-6-FAILOVER_REQ: Stack-unit failover
request from active peer: User request.
Jul 30 16:31:33: %PE255-UNIT3-M:CP %CHMGR-4-TEMP_STATUS_CHANGE: Unit 2
```

```
temperature state changed to 1 (Current temperature 36C).
Jul 30 16:31:33: %PE-UNKN-C1048P:2 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 75 % of the full speed
Jul 30 16:31:32: %PE255-UNIT3-M:CP %IFMGR-5-OSTATE_UP: Changed interface state
to up: Te 2/1
Jul 30 16:31:32: %PE-UNKN-C1048P:2 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 60 % of the full speed
Jul 30 16:31:32: %PE255-UNIT3-M:CP %CHMGR-5-FANTRAY_INSERTED: Fan tray 0 of
Unit 2 is inserted
Jul 30 16:31:32: %PE-UNKN-C1048P:2 %CHMGR-2-FAN_SPEED_CHANGE: Fan speed
changed to 60 % of the full speed
Jul 30 16:31:32: %PE255-UNIT3-M:CP %CHMGR-0-PS_DOWN: Major alarm: Power supply
1 in unit 2 is down
Jul 30 16:31:32: %PE255-UNIT3-M:CP %CHMGR-5-PEM_INSERTED: Power entry module 1
of unit 2 is inserted
Jul 30 16:31:32: %PE255-UNIT3-M:CP %CHMGR-0-PS_UP: Power supply 0 in unit 2 is
up
Jul 30 16:31:32: %PE255-UNIT3-M:CP %CHMGR-5-PEM_INSERTED: Power entry module 0
of unit 2 is inserted
Jul 30 16:31:25: %PE-UNKN-C1048P:2 %IFAGT-5-INSERT_OPTICS_PLUS: Optics SFP+
inserted in slot 2 port 1
Jul 30 16:31:25: %PE-UNKN-C1048P:2 %IFAGT-5-STACK_PORT_LINK_UP: Changed stack
port state to up: 2/2
Jul 30 16:31:25: %PE-UNKN-C1048P:2 %IFAGT-5-STACK_PORT_LINK_UP: Changed stack
port state to up: 2/1
Jul 30 16:31:24: %PE255-UNIT3-M:CP %CHMGR-5-STACKUNIT_UP: stack-unit 2 is up
Jul 30 16:31:23: %PE255-UNIT3-M:CP %CHMGR-5-CHECKIN: Checkin from stack-unit 2
(type C1048P, 52 ports)
Jul 30 16:31:21: %PE255-UNIT3-M:CP %CHMGR-5-STACKUNIT_DETECTED: stack-unit 2
present
Jul 30 16:31:13: %PE255-UNIT1-S:CP %EVL-6-EVENT_LOGGING: Completed uploading
pre-recorded traps(send count:3, pending traps:0) to CB
Jul 30 16:31:13: %PE255-UNIT1-S:CP %EVL-6-EVENT_LOGGING: Start uploading pre-
recorded traps(count:3) to CB
Jul 30 16:31:11: %PE255-C1048P:3 %IFAGT-5-STACK_PORT_LINK_UP: Changed stack
port state to up: 3/2
Jul 30 16:31:11: %PE255-C1048P:1 %IFAGT-5-STACK_PORT_LINK_UP: Changed stack
port state to up: 1/1
Jul 30 16:31:11: %PE-UNKN-UNIT1-S:CP %RAM-5-STACKUNIT_STATE: Stack-unit 1 is
in Standby State.
Jul 30 16:31:06: %PE-UNKN-UNIT1-S:CP %POLLMGR-2-ALT_STACKUNIT_STATE: Alternate
Stack-unit is present
Jul 30 16:31:06: %PE-UNKN-UNIT1-U:CP %RAM-6-ELECTION_ROLE: Stack-unit 1 is
transitioning to Standby Stack-unit.
Jul 30 16:31:06: %PE-UNKN-UNIT1-U:CP %IRC-6-IRC_COMMUP: Link to peer Stack-
unit is up
```

```
Dell#show logging 1
Syslog logging: enabled
    Console logging: level debugging
    Monitor logging: level debugging
    Buffer logging: level debugging, 33 Messages Logged, Size (40960 bytes)
    Trap logging: level informational
Jul 7 14:20:19: %PE1-UNIT1-M:CP %SEC-5-LOGIN_SUCCESS: Login successful on
console
```

show logging auditlog

Displays an audit log.

C9000 Series

Syntax `show logging auditlog`

Defaults none

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL.

Example

```
Dell(conf)#show logging audit
```

Related Commands clear logging auditlog — clears audit log.

show logging driverlog

Display the driver log for the specified hardware component.

C9000 Series

Syntax `show logging driverlog {cp | linecard slot-id | pe pe-id stack–unit unit number`

From a **PE console**, use the `show logging driverlog stack–unit unit number` to view the driver logging information for a specified stack-unit.

Parameters

cp	Enter the keyword `cp` to display the driver log for the Control Processor on the switch.
linecard *slot-id*	Enter the `linecard slot-id` parameters to specify the line-card ports for which you want to display the driver log. The range of line-card slot IDs is from 0 to 11.
pe *pe-id*	Enter the keyword `pe` and the port extender ID to display the driver log information for the specified port extender. Port extender ID range is from 0 to 255.
stack *unit-number*	Enter the keyword `stack-unit` and the unit number to display the driver log information for the specified stack-unit. Stack unit range is from 0 to 7.

defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Usage Information

This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors.

Examples

```
Dell# show logging driverlog cp
0:Task(dlm): [  6472921]EEPROM LIB ERR: decipherPpId:349 PPID ERROR:
Mismatching VID and MFGID

1:Task(dlm): [      101]EEPROM LIB ERR: decipherPpId:379 Invalid svcTag(n/a)
2:Task(dlm): [       93]EEPROM LIB ERR: decipherPpId:390 strtoull invalidates
svcTag(n/a): errno(0), *enr(/)
3:Task(dlm): [       40]EEPROM LIB ERR: decipherPpId:416 svcTag invalid
changing it to NA
4:Task(chmgr): [  1555744]EEPROM LIB ERR: decipherPpId:349 PPID ERROR:
Mismatching VID and MFGID
5:Task(chmgr): [       50]EEPROM LIB ERR: decipherPpId:379 Invalid svcTag(n/a)
6:Task(chmgr): [       42]EEPROM LIB ERR: decipherPpId:390 strtoull
invalidates svcTag(n/a): errno(0), *ptr(/)
7:Task(chmgr): [       39]EEPROM LIB ERR: decipherPpId:416 svcTag invalid
changing it to NA


Dell# show logging driverlog linecard 0

0:Task(tUsrRoot): [    29525]SS DRV DEBUG: Wrapper init complete
1:Task(tUsrRoot): [   301305]SS DRV DEBUG: Core init complete
2:Task(tUsrRoot): [      913]SS DRV DEBUG: port:0 isfanout:0
3:Task(tUsrRoot): [       40]SS DRV DEBUG: port:4 isfanout:0
4:Task(tUsrRoot): [       36]SS DRV DEBUG: port:8 isfanout:0
5:Task(tUsrRoot): [       36]SS DRV DEBUG: port:12 isfanout:0
6:Task(tUsrRoot): [       36]SS DRV DEBUG: port:16 isfanout:0
7:Task(tUsrRoot): [       36]SS DRV DEBUG: port:20 isfanout:0
8:Task(tUsrRoot): [       36]SS DRV DEBUG: port:24 isfanout:0
9:Task(tUsrRoot): [       36]SS DRV DEBUG: port:28 isfanout:0
10:Task(tUsrRoot): [       35]SS DRV DEBUG: port:32 isfanout:0
```

Example (PE Console)

```
Dell#show logging driverlog  stack-unit 1
0:Task(tUsrRoot): [   655621]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom: Main
block failed checksum calulated checksum 0x1d32 actual chksum 0x0

1:Task(tUsrRoot): [      425]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom: Main
block failed errcode 6

2:Task(tUsrRoot): [       71]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed checksum calulated checksum 0x3e4b actual chksum 0x0

3:Task(tUsrRoot): [       55]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed errcode 6

4:Task(tUsrRoot): [       50]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom,
failed to get any good block

5:Task(tUsrRoot): [       74]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom: Main
```

```
block failed checksum calulated checksum 0x1d32 actual chksum 0x0

6:Task(tUsrRoot): [       55]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom: Main
block failed errcode 6

7:Task(tUsrRoot): [       60]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed checksum calulated checksum 0x3e4b actual chksum 0x0

8:Task(tUsrRoot): [       55]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed errcode 6

9:Task(tUsrRoot): [       49]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom,
failed to get any good block

10:Task(tUsrRoot): [      782]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Main block failed checksum calulated checksum 0x1d32 actual chksum 0x0

11:Task(tUsrRoot): [     1878]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Main block failed errcode 6

12:Task(tUsrRoot): [       71]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed checksum calulated checksum 0x3e4b actual chksum 0x0

13:Task(tUsrRoot): [       56]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed errcode 6

14:Task(tUsrRoot): [       86]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom,
failed to get any good block

15:Task(tUsrRoot): [       77]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Main block failed checksum calulated checksum 0x1d32 actual chksum 0x0

16:Task(tUsrRoot): [       54]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Main block failed errcode 6

17:Task(tUsrRoot): [       62]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed checksum calulated checksum 0x3e4b actual chksum 0x0

18:Task(tUsrRoot): [       53]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed errcode 6

19:Task(tUsrRoot): [       49]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom,
failed to get any good block

20:Task(tUsrRoot): [       71]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Main block failed checksum calulated checksum 0x1d32 actual chksum 0x0

21:Task(tUsrRoot): [       52]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Main block failed errcode 6

22:Task(tUsrRoot): [       61]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed checksum calulated checksum 0x3e4b actual chksum 0x0

23:Task(tUsrRoot): [       53]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed errcode 6

24:Task(tUsrRoot): [       49]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom,
failed to get any good block

25:Task(tUsrRoot): [       70]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Main block failed checksum calulated checksum 0x1d32 actual chksum 0x0

26:Task(tUsrRoot): [       53]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Main block failed errcode 6

27:Task(tUsrRoot): [       61]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
Redundant block failed checksum calulated checksum 0x3e4b actual chksum 0x0

28:Task(tUsrRoot): [       53]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom:
```

```
Redundant block failed errcode 6

29:Task(tUsrRoot): [       49]EEPROM LIB ERR: f10EepromBlkRead@psu0eeprom,
failed to get any good block

30:Task(tUsrRoot): [       61]EEPROM LIB ERR: decipherPpId:371 Invalid ppId[]
size[0]
31:Task(tUsrRoot): [     9251]31:SS DRV DEBUG: bcmDrvCardShortId is 0x8880
32:Task(tUsrRoot): [   479623]32:SS DRV DEBUG: No.of Device Got Attached 1
33:Task(tUsrRoot): [       86]32:SS DRV DEBUG: bcmDrvUpdatePortTable complete
for unit 0
34:Task(tUsrRoot): [       67]32:SS DRV DEBUG: bcmDrvHelixPortTblInit -
complete for unit 0
35:Task(tUsrRoot): [       63]32:SS DRV DEBUG: Updating based on Fanout
36:Task(tUsrRoot): [       75]32:SS DRV DEBUG: nv sysdlp fan out NVID open
failed
37:Task(tUsrRoot): [       53]SS DRV ERR: Updating port tbl from fanout failed
38:Task(tUsrRoot): [       54]32:SS DRV DEBUG: Updating based on Stacking
39:Task(tUsrRoot): [     9842]32:SS DRV DEBUG: Updating device entry from port
table
40:Task(tUsrRoot): [    19716]32:SS DRV DEBUG: Sysconf attach complete
41:Task(tUsrRoot): [   697608]33:SS DRV DEBUG: Unit 0 : Soc Reset Complete
42:Task(tUsrRoot): [   693327]33:SS DRV DEBUG: Unit 0 : Soc Misc Init Complete
43:Task(tUsrRoot): [   770793]34:SS DRV DEBUG: Unit 0 : Soc MMU Init Complete
44:Task(tUsrRoot): [  4455907]38:SS DRV DEBUG: Unit 0 : Soc BCM INitComplete
45:Task(tUsrRoot): [       81]38:SS DRV DEBUG: Unit 0: Basic Inits complete
46:Task(tUsrRoot): [    32839]39:SS DRV DEBUG:
bcmDrvSwitchTypeChipInitSettings complete for unit 0
47:Task(tUsrRoot): [   127018]39:SS DRV DEBUG: Initializing Stack port unit 0
port 54
48:Task(tUsrRoot): [   200703]39:SS DRV DEBUG: Initializing Stack port unit 0
port 55
49:Task(tUsrRoot): [   199953]39:SS DRV DEBUG: Port Setup Done
50:Task(tUsrRoot): [  2938047]42:SS DRV DEBUG: QOS Setup Done
51:Task(tUsrRoot): [   232921]SS DRV ERR:  BCM API Invocation Error(Vlan
already Exists) - Error(-8, Entry exists)
52:Task(tUsrRoot): [   590818]43:SS DRV DEBUG: S_SERIES_STACK: Waiting on
stack discovery
53:Task(tUsrRoot): [  8680680]51:SS DRV DEBUG: bcmDrvPostSettings Setup Done
54:Task(tUsrRoot): [      562]========================================
55:Task(tUsrRoot): [       51]sysDrvLoggerFreezeTop: Top of Log Frozen.
56:Task(tUsrRoot): [       40]===== FREEZE BY REQUEST ==================
57:Task(tUsrRoot): [       39]========================================
58:Task(tUsrRoot): [       53]51:SS DRV DEBUG: bcmDrvInit Done
59:Task(tUsrRoot): [       67]51:SS DRV DEBUG: bcmDrvInit: Returning, Time
taken 20131916 micro-secs
60:Task(ifagt_1): [  3447148]SS DRV ERR:  BCM API Invocation
Error(bcm_phy84740_pmad_reg_get failed
61:Task(ifagt_1): [  1070425]SS DRV ERR:  BCM API Invocation
Error(bcm_phy84740_pmad_reg_get failed  (<- repeated 9 times)
62:Task(ifagt_1): [  1070425]56:SS DRV DEBUG:
halOpticsUpdateSerialIdInfoUpdate: Update Serial ID Info for XFP48
63:Task(envmgr): [  1561704]EEPROM LIB ERR: decipherPpId:371 Invalid ppId[]
size[0]
64:Task(ifagt_1): [ 3351519774]EEPROM LIB ERR: decipherPpId:371 Invalid ppId[]
size[0]  (<- repeated 1 times)
65:Task(ifagt_1): [ 3351519774]SS DRV ERR:  BCM API Invocation
Error(bcm_phy84740_pmad_reg_get failed
```

show logging kernellog

Display the kernel log for the specified hardware component.

C9000 Series

Syntax

`show logging kernellog {cp | rp | linecard` *`slot-id`* `| pe` *`pe-id`* `stack unit` *`unit-number`*`}`

From a **PE console**, use `show logging kernellog stack-unit` *`unit number`* to display the kernel logging information for a specified stack-unit.

Parameters

cp	Enter the keyword `cp` to display the kernel log for the Control Processor on the switch.
rp	Enter the keyword `cp` to display the kernel log for the Route Processor on the switch.
linecard *slot-id*	Enter the `linecard` *`slot-id`* parameters to specify the line-card ports for which you want to display the kernel log. The range of line-card slot IDs is from 0 to 2.
pe *pe-id*	Enter the keyword `pe` and the port extender the ID to display the kernel log for the specified port extender. The PE ID range is from 0 to 255.
stack unit *unit number*	Enter keyword `stack-unit` and the stack-unit number to display the kernel log for the specified stack unit. Stack-unit number range is from 0 to 7.

defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11(0.0)	Introduced on N20xx and N30xx series.
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.

Usage Information

This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed port pipe.

In a dual homing setup, you can use this command only from the primary VLT peer.

Examples

```
Dell# show logging kernellog cp
00:00:02:326592:AHCI_P_SCTL(0x01ac)     0x00000300
00:00:02:326599:AHCI_P_SERR(0x01b0)     0x00000000
00:00:02:326605:AHCI_P_SACT(0x01b4)     0x00000000
00:00:02:655656:pca9555x3:pca9555_write: iic_smbus_write_byte failed addr=0x20
cmd_reg=0x8 rv=5
00:00:02:656982:pca9555x3:pca9555_write: iic_smbus_write_byte failed addr=0x20
cmd_reg=0x9 rv=5
00:00:02:659597:pca9555x3:pca9555_write: iic_smbus_write_byte failed addr=0x20
cmd_reg=0xf rv=5
00:00:43:418634:PCI unit 0: Dev 0xb852, Rev 0x03, Chip BCM56852_A2, Driver
BCM56850_A0
00:00:43:418655:PCI unit 1: Dev 0xb852, Rev 0x03, Chip BCM56852_A2, Driver
BCM56850_A0
00:00:43:418671:PCI unit 2: Dev 0xb852, Rev 0x03, Chip BCM56852_A2, Driver
BCM56850_A0
00:00:43:418687:PCI unit 3: Dev 0xb852, Rev 0x03, Chip BCM56852_A2, Driver
BCM56850_A0
00:00:43:418702:PCI unit 4: Dev 0xb852, Rev 0x03, Chip BCM56852_A2, Driver
BCM56850_A0
00:00:43:418718:PCI unit 5: Dev 0xb852, Rev 0x03, Chip BCM56852_A2, Driver
BCM56850_A0
00:00:43:418732:PCI unit 6: Dev 0xb636, Rev 0x11, Chip BCM56636_B0, Driver
BCM56634_B0

Dell#show logging kernellog rp
00:00:01:918834:ahcisata0 port 0: device present, speed: 6.0Gb/s
00:00:02:919154:ahcisata0 port 1: device not present
00:00:02:919164:
AHCI Global register dump
00:00:02:919171:AHCI_CAP(0x0000)        0xe237ff21
00:00:02:919178:AHCI_GHC(0x0004)        0x80000002
00:00:02:919184:AHCI_IS(0x0008) 0x00000000
00:00:02:919190:AHCI_PI(0x000c) 0x00000003
00:00:02:919197:AHCI_VS(0x0010) 0x00010000
00:00:02:919204:AHCI_CC_CTL(0x0014)     0x00010120
00:00:02:919210:AHCI_CC_PORTS(0x0018)   0x00000000
00:00:02:919217:AHCI_EM_LOC(0x001c)     0x00000000
00:00:02:919223:AHCI_EM_CTL(0x0020)     0x00000000
00:00:02:919229:AHCI per port register dump for port 1
00:00:02:919236:AHCI_P_IS(0x0190)       0x00000000
00:00:02:919243:AHCI_P_IE(0x0194)       0x00000000
00:00:02:919249:AHCI_P_CLBU(0x0184)     0x00000000
00:00:02:919255:AHCI_P_CLB(0x0180)      0x06491400
00:00:02:919262:AHCI_P_FBU(0x018c)      0x00000000
00:00:02:919269:AHCI_P_FB(0x0188)       0x06491900
00:00:02:919275:AHCI_P_CMD(0x0198)      0x00700016
00:00:02:919282:AHCI_P_CI(0x01b8)       0x00000000
00:00:02:919288:AHCI_P_TFD(0x01a0)      0x0000007f
00:00:02:919295:AHCI_P_SIG(0x01a4)      0xffffffff
00:00:02:919302:AHCI_P_SSTS(0x01a8)     0x00000000
00:00:02:919308:AHCI_P_SCTL(0x01ac)     0x00000300
00:00:02:919315:AHCI_P_SERR(0x01b0)     0x00000000
00:00:02:919321:AHCI_P_SACT(0x01b4)     0x00000000

Dell#show logging kernellog linecard 0
1d 02:24:49:841597:qsfp-3 eeprom attempting to read on from iic at : 14
1d 02:24:49:849249:qsfp-6 eeprom attempting to read on from iic at : 24
1d 02:24:49:856820:qsfp-7 eeprom attempting to read on from iic at : 23
1d 02:24:49:872175:qsfp-11 eeprom attempting to read on from iic at : 18
1d 02:26:50:140882:qsfp-0 eeprom attempting to read on from iic at : 17
1d 02:26:50:148668:qsfp-1 eeprom attempting to read on from iic at : 16
1d 02:26:50:156237:qsfp-2 eeprom attempting to read on from iic at : 15
1d 02:26:50:163966:qsfp-3 eeprom attempting to read on from iic at : 14
1d 02:26:50:179846:qsfp-6 eeprom attempting to read on from iic at : 24
1d 02:26:50:187498:qsfp-7 eeprom attempting to read on from iic at : 23
```

```
1d 02:26:50:202989:qsfp-11 eeprom attempting to read on from iic at : 18
1d 02:28:50:440146:qsfp-0 eeprom attempting to read on from iic at : 17
1d 02:28:50:447933:qsfp-1 eeprom attempting to read on from iic at : 16
1d 02:28:50:455505:qsfp-2 eeprom attempting to read on from iic at : 15
1d 02:28:50:463233:qsfp-3 eeprom attempting to read on from iic at : 14
1d 02:28:50:470881:qsfp-6 eeprom attempting to read on from iic at : 24
1d 02:28:50:478591:qsfp-7 eeprom attempting to read on from iic at : 23
1d 02:28:50:493790:qsfp-11 eeprom attempting to read on from iic at : 18
1d 02:30:50:675435:qsfp-0 eeprom attempting to read on from iic at : 17
1d 02:30:50:683019:qsfp-1 eeprom attempting to read on from iic at : 16
```

Example ((PE Console)

```
Dell#show logging kernellog stack-unit 1
00:00:32:342561:AXI unit 0: Dev 0xb340, Rev 0x01, Chip BCM56340_A0, Driver
BCM56340_A0
```

terminal monitor

Configure the system to display messages on the monitor/terminal.

C9000 Series

Syntax

`terminal monitor`

To return to default settings, use the `terminal no monitor` command.

defaults

Disabled.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Related Commands

logging monitor — sets the logging parameters on the monitor/terminal.

57

SNMP Traps

This chapter lists the traps sent by the Dell Networking operating software. Each trap is listed by the fields Message ID, Trap Type, and Trap Option.

Table 13. SNMP Trap List

Message ID	Trap Type	Trap Option
COLD_START	SNMP	COLDSTART
`%SNMP-5-SNMP_COLD_START: SNMP COLD_START trap sent.`		
WARM_START	SNMP	WARMSTART
COPY_CONFIG_COMPLETE	SNMP	NONE
`SNMP Copy Config Command Completed`		
LINK_DOWN	SNMP	LINKDOWN
`%IFA-1-PORT_LINKDN: changed interface state to down:%d`		
LINK_UP	SNMP	LINKUP
`%IFA-1-PORT_LINKUP: changed interface state to up:%d`		
AUTHENTICATION_FAIL	SNMP	AUTH
`%SNMP-3-SNMP_AUTH_FAIL: SNMP Authentication failed.Request with invalid community string.`		
EGP_NEIGHBOR_LOSS	SNMP	NONE
OSTATE_DOWN	SNMP	LINKDOWN
`%IFM-1-OSTATE_DN: changed interface state to down:%s`		
`%IFM-5-CSTATE_DN:Changed interface Physical state to down: %s`		
OSTATE_UP	SNMP	LINKUP
`%IFM-1-OSTATE_UP: changed interface state to up:%s`		
`%IFM-5-CSTATE_UP: Changed interface Physical state to up: %s`		
RMON_RISING_THRESHOLD	SNMP	NONE
`%RPM0-P:CP %SNMP-4-RMON_RISING_THRESHOLD: RMON rising threshold alarm from SNMP OID <oid>`		
RMON_FALLING_THRESHOLD	SNMP	NONE
`%RPM0-P:CP %SNMP-4-RMON_FALLING_THRESHOLD: RMON falling threshold alarm from SNMP OID <oid>`		
RMON_HC_RISHING_THRESHOLD	SNMP	NONE
`%RPM0-P:CP %SNMP-4-RMON_HC_RISING_THRESHOLD: RMON high-capacity rising threshold alarm from SNMP OID <oid>`		
RMON_HC_FALLING_THRESHOLD	SNMP	NONE

Message ID	Trap Type	Trap Option
%RPM0-P:CP %SNMP-4-RMON_HC_FALLING_THRESHOLD: RMON high-capacity falling threshold alarm from SNMP OID <oid>		
BER_ERR	SNMP	NONE
%IFMGR-5-BER_ERR: High Ber detected on interface : %s		
BER_ERR_CLR	SNMP	NONE
%IFMGR-5-BER_ERR_CLR: High Ber cleared on interface : %s		
FAST_RETRAIN	SNMP	NONE
%IFMGR-5-FAST_RETRAIN: Retrain event detected on interface : %s		
RESV	NONE	NONE
N/A		
CHM_CARD_DOWN	ENVMON	NONE
%CHMGR-1-CARD_SHUTDOWN: %sLine card %d down - %s		
%CHMGR-2-CARD_DOWN: %sLine card %d down - %s		
CHM_CARD_UP	ENVMON	NONE
%CHMGR-5-LINECARDUP: %sLine card %d is up		
CHM_CARD_MISMATCH	ENVMON	NONE
%CHMGR-3-CARD_MISMATCH: Mismatch: line card %d is type %s - type %s required.		
CHM_CARD_PROBLEM	ENVMON	NONE
CHM_ALARM_CUTOFF	ENVMON	NONE
CHM_SFM_UP	ENVMON	NONE
CHM_SFM_DOWN	ENVMON	NONE
CHM_RPM_UP	ENVMON	NONE
%RAM-6-RPM_STATE: RPM1 is in Active State		
%RAM-6-RPM_STATE: RPM0 is in Standby State		
CHM_RPM_DOWN	ENVMON	NONE
%CHMGR-2-RPM_DOWN: RPM 0 down - hard reset		
%CHMGR-2-RPM_DOWN: RPM 0 down — card removed		
CHM_RPM_PRIMARY	ENVMON	NONE
%RAM-5-COLD_FAILOVER: RPM Failover Completed		
%RAM-5-HOT_FAILOVER: RPM Failover Completed		
%RAM-5-FAST_FAILOVER: RPM Failover Completed		
CHM_SFM_ADD	ENVMON	NONE
%TSM-5-SFM_DISCOVERY: Found SFM 1		

Message ID	Trap Type	Trap Option
CHM_SFM_REMOVE	ENVMON	NONE
%TSM-5-SFM_REMOVE: Removed SFM 1		
CHM_MAJ_SFM_DOWN	ENVMON	NONE
%CHMGR-0-MAJOR_SFM: Major alarm: Switch fabric down		
CHM_MAJ_SFM_DOWN_CLR	ENVMON	NONE
%CHMGR-5-MAJOR_SFM_CLR: Major alarm cleared: Switch fabric up		
CHM_MIN_SFM_DOWN	ENVMON	NONE
%CHMGR-2-MINOR_SFM: MInor alarm: No working standby SFM		
CHM_MIN_SFM_DOWN_CLR	ENVMON	NONE
%CHMGR-5-MINOR_SFM_CLR: Minor alarm cleared: Working standby SFM present		
CHM_PWRSRC_DOWN	ENVMON	SUPPLY
%CHMGR-2-PEM_PRBLM: Major alarm: problem with power entry module %s		
CHM_PWRSRC_CLR	ENVMON	SUPPLY
%CHMGR-5-PEM_OK: Major alarm cleared: power entry module %s is good		
CHM_MAJ_ALARM_PS	ENVMON	SUPPLY
%CHMGR-0-MAJOR_PS: Major alarm: insufficient power %s		
CHM_MAJ_ALARM_PS_CLR	ENVMON	SUPPLY
%CHMGR-5-MAJOR_PS_CLR: major alarm cleared: sufficient power		
CHM_MIN_ALARM_PS	ENVMON	SUPPLY
%CHMGR-1-MINOR_PS: Minor alarm: power supply non-redundant		
CHM_MIN_ALARM_PS_CLR	ENVMON	SUPPLY
%CHMGR-5-MINOR_PS_CLR: Minor alarm cleared: power supply redundant		
CHM_MIN_ALRM_TEMP	ENVMON	TEMP
%CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature		
CHM_MIN_ALRM_TEMP_CLR	ENVMON	TEMP
%CHMRG-5-MINOR_TEMP_CLR: Minor alarm cleared: chassis temperature normal (%s %d temperature is within threshold of %dC)		
CHM_MAJ_ALRM_TEMP	ENVMON	TEMP
%CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s temperature reaches or exceeds threshold of %dC)		
CHM_MAJ_ALRM_TEMP_CLR	ENVMON	TEMP
%CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: chassis temperature lower (%s %d temperature is within threshold of %dC)		
CHM_FANTRAY_BAD	ENVMON	FAN

Message ID	Trap Type	Trap Option
For E1200: %CHMGR-2-FAN_TRAY_BAD: Major alarm: fan tray %d is missing or down %CHMGR-2-ALL_FAN_BAD: Major alarm: all fans in fan tray %d are down. For E600 and E300: %CHMGR-2-FANTRAYBAD: Major alarm: fan tray is missing %CHMGR-2-FANSBAD: Major alarm: most or all fans in fan tray are down		
CHM_FANTRAY_BAD_CLR For the E1200: %CHMGR-5-FAN_TRAY_OK: Major alarm cleared: fan tray %d present For the E600 and E300: %CHMGR-5-FANTRAYOK: Major alarm cleared: fan tray present	ENVMON	FAN
CHM_MIN_FANBAD For the E1200: %CHMGR-2-FAN_BAD: Minor alarm: some fans in fan tray %d are down For the E600 and E300: %CHMGR- 2-1FANBAD: Minor alarm: fan in fan tray is down	ENVMON	FAN
CHM_MIN_FANBAD_CLR For E1200: %CHMGR-2-FAN_OK: Minor alarm cleared: all fans in fan tray %d are good For E600 and E300: %CHMGR-5-FANOK: Minor alarm cleared: all fans in fan tray are good	ENVMON	FAN
TME_TASK_SUSPEND %TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s	ENVMON	NONE
TME_TASK_TERM %TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s	ENVMON	NONE
CHM_CPU_THRESHOLD %CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)	ENVMON	NONE
CHM_CPU_THRESHOLD_CLR %CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)	ENVMON	NONE
CHM_MEM_THRESHOLD %CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)	ENVMON	NONE
CHM_MEM_THRESHOLD_CLR %CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)	ENVMON	NONE
MACMGR_STN_MOVE	ENVMON	NONE

Message ID	Trap Type	Trap Option
%MACMGR-5-DETECT_STN_MOVE: Station Move threshold exceeded for Mac %s in vlan %d		
PORT_TEMP_MAJOR	ENVMON	NONE
%CHMGR-1-PORT_TEMP_MAJOR: Major Alarm Interface %s shut due to high temperature		
PORT_TEMP_MINOR	ENVMON	NONE
%CHMGR-1-PORT_TEMP_MINOR: Minor Alarm Interface %s temperature exceeds threshold		
PORT_TEMP_MAJOR_CLR	ENVMON	NONE
%CHMGR-1-PORT_TEMP_MAJOR_CLR: Major Alarm cleared for Interface %s port temperature is lower than threshold		
VRRP_BADAUTH	PROTO	NONE
%RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication type mismatch. %RPM1-P:RP2 %VRRP-3-VRRP_BAD_AUTH: vrid-1 on Gi 11/12 rcvd pkt with authentication failure		
VRRP_GO_MASTER	PROTO	NONE
%VRRP-6-VRRP_MASTER: vrid-%d on %s entering MASTER		
VRRP_PROTOCOL_ERROR	PROTO	NONE
VRRP_PROTOERR: VRRP protocol error on %S		
BGP4_ESTABLISHED	PROTO	NONE
%TRAP-5-PEER_ESTABLISHED: Neighbor %a, state %s		
BGP4_BACKW_XSITION	PROTO	NONE
%TRAP-5-BACKWARD_STATE_TRANS: Neighbor %a, state %s		
CH_ALARM_CARD_DOWN	ENVMON	NONE
%PE0-UNIT0-M%STACKUNIT_DOWN: Major alarm cleared: stack-unit 0 down - auto-shutdown due to high heat		
CH_ALARM_TASK_SUSPEND	ENVMON	NONE
%PE100-UNIT0-M%TASK SUSPENDED: SUSPENDED - svce:13 - inst:0 - task:tme		
CH_ALARM_TASK_TERM	ENVOM	NONE
%PE100-UNIT0-M%ABNORMAL_TASK_TERMINATION: CRASH - task:tme Svce:13 - Inst:0		
CH_ALARM_EXD_CPU_THRESHOLD	ENVMON	NONE
%PE8-UNIT0-M%CPU_THRESHOLD: Overall cpu usage of cp is above threshold. Cpu5secUsage (95%)		
CH_ALARM_CLR_CPU_THRESHOLD	ENVMON	NONE
%PE8-UNIT0-M%CPU_THRESHOLD_CLR: Overall cpu usage of cp drops below threshold. Cpu5secUsage (10%)		
CH_ALARM_EXD_MEM_THRESHOLD	ENVMON	NONE
%PE8-UNIT0-M%MEM_THRESHOLD: Overall memory usage of cp is above threshold. Memory Usage (80%)		

Message ID	Trap Type	Trap Option
CH_ALARM_CLR_MEM_THRESHOLD	ENVMON	NONE
%PE8-UNIT0-M%MEM_THRESHOLD_CLR: Overall memory usage of cp drops below threshold. Memory Usage (20%)		
CH_ALARM_PE_DOWN	DOT1BR	NONE
PE_DOWN: PE:6 MAC:00:01:02:03:04:05 is operationally down.		
CH_ALARM_PE_UP	DOT1BR	NONE
PE_UP: PE:6 MAC:00:01:02:03:04:05 is operationally up.		
CH_ALARM_PE_UNIT_DOWN	DOT1BR	NONE
PE_UNIT_DOWN: PE:6 Unit:0 Unit MAC:00:01:02:03:04:05 operationally down.		
CH_ALARM_PE_UNIT_UP	DOT1BR	NONE
PE_UNIT_UP: PE:6 Unit:0 Unit MAC:00:01:02:03:04:05 operationally up.		
PE0-UNIT0-M%FAN_BAD_CLR: Minor alarm cleared: Alarm, 1 out of 2 fans in fantray 0 down, reported for unit 2 is cleared		
PE0-UNIT0-M%ALL_FAN_BAD: Major alarm: all fans in fantray 0 of unit 0 are down		

58

Spanning Tree Protocol (STP)

The commands in this chapter configure and monitor the IEEE 802.1d spanning tree protocol (STP).

Topics:

- bpdu-destination-mac-address
- bridge-priority
- debug spanning-tree
- description
- disable
- forward-delay
- hello-time
- max-age
- protocol spanning-tree
- show config
- show spanning-tree 0
- spanning-tree 0

bpdu-destination-mac-address

Use the Provider Bridge Group address in Spanning Tree or GVRP PDUs.

C9000 Series

Syntax `bpdu-destination-mac-address [stp | gvrp] provider-bridge-group`

Parameters

xstp	Force STP, RSTP, and MSTP to use the Provider Bridge Group address as the destination MAC address in its BPDUs.
gvrp	Forces GVRP to use the Provider Bridge GVRP Address as the destination MAC address in its PDUs.

Defaults The destination MAC address for BPDUs is the Bridge Group Address.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the S4810.
8.2.1.0	Introduced on the C-Series and S-Series.

bridge-priority

Set the bridge priority of the switch in an IEEE 802.1D spanning tree.

C9000 Series

Syntax

`bridge-priority {`*`priority-value`* `| primary | secondary}`

To return to the default value, use the `no bridge-priority` command.

Parameters

priority-value	Enter a number as the bridge priority value. The range is from 0 to 65535. The default is **32768**.
primary	Enter the keyword `primary` to designate the bridge as the root bridge.
secondary	Enter the keyword `secondary` to designate the bridge as a secondary root bridge.

Defaults

priority-value = **32768**

Command Modes

SPANNING TREE (The prompt is "config-stp".)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

debug spanning-tree

Enable debugging of the spanning tree protocol and view information on the protocol.

C9000 Series

Syntax

```
debug spanning-tree {stp-id [all | bpdu | config | events | exceptions | general | root] | protocol}
```

To disable debugging, use the `no debug spanning-tree` command.

Parameters

stp-id	Enter zero (0). The switch supports one spanning tree group with a group ID of 0.
protocol	Enter the keyword for the type of STP to debug, either `mstp`, `pvst`, or `rstp`.
all	(OPTIONAL) Enter the keyword `all` to debug all spanning tree operations.
bpdu	(OPTIONAL) Enter the keyword `bpdu` to debug bridge protocol data units.
config	(OPTIONAL) Enter the keyword `config` to debug configuration information.
events	(OPTIONAL) Enter the keyword `events` to debug STP events.
general	(OPTIONAL) Enter the keyword `general` to debug general STP operations.
root	(OPTIONAL) Enter the keyword `root` to debug STP root transactions.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information When you enable `debug spanning-tree bpdu` for multiple interfaces, the software only sends information on BPDUs for the last interface specified.

Related Commands protocol spanning-tree — enters SPANNING TREE mode on the switch.

description

Enter a description of the spanning tree.

C9000 Series

Syntax

`description {description}`

To remove the description from the spanning tree, use the `no description {description}` command.

Parameters

description	Enter a description to identify the spanning tree (80 characters maximum).

Defaults

none

Command Modes

SPANNING TREE (The prompt is "config-stp".)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced

Related Commands

protocol spanning-tree — enters SPANNING TREE mode on the switch.

disable

Disable the spanning tree protocol globally on the switch.

C9000 Series

Syntax

`disable`

To enable Spanning Tree Protocol, use the `no disable` command.

Defaults

Enabled (that is, the spanning tree protocol is disabled.)

Command Modes

SPANNING TREE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands protocol spanning-tree — enters SPANNING TREE mode on the switch.

forward-delay

The amount of time the interface waits in the Listening state and the Learning state before transitioning to the Forwarding state.

C9000 Series

Syntax `forward-delay` *seconds*

To return to the default setting, use the `no forward-delay` command.

Parameters

seconds	Enter the number of seconds the system waits before transitioning STP to the Forwarding state. The range is from 4 to 30. The default is **15 seconds**.

Defaults **15 seconds**

Command Modes SPANNING TREE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands max-age — changes the wait time before STP refreshes protocol configuration information.

hello-time — changes the time interval between BPDUs.

hello-time

Set the time interval between generation of the spanning tree bridge protocol data units (BPDUs).

C9000 Series

Syntax `hello-time seconds`

To return to the default value, use the `no hello-time` command.

Parameters

seconds	Enter a number as the time interval between transmission of BPDUs. The range is from 1 to 10. The default is **2 seconds**.

Defaults **2 seconds**

Command Modes SPANNING TREE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands forward-delay — changes the wait time before STP transitions to the Forwarding state.

max-age — changes the wait time before STP refreshes protocol configuration information.

max-age

To maintain configuration information before refreshing that information, set the time interval for the spanning tree bridge.

C9000 Series

Syntax

```
max-age seconds
```

To return to the default values, use the `no max-age` command.

Parameters

seconds	Enter a number of seconds the system waits before refreshing configuration information. The range is from 6 to 40. The default is **20 seconds**.

Defaults **20 seconds**

Command Modes SPANNING TREE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Related Commands forward-delay — changes the wait time before STP transitions to the Forwarding state.

hello-time — changes the time interval between BPDUs.

protocol spanning-tree

To enable and configure the spanning tree group, enter SPANNING TREE mode.

C9000 Series

Syntax

```
protocol spanning-tree stp-id
```

To disable the Spanning Tree group, use the `no protocol spanning-tree stp-id` command.

Parameters

stp-id	Enter zero (0). the system supports one spanning tree group, group 0.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information STP is not enabled when you enter SPANNING TREE mode. To enable STP globally on the switch, use the `no disable` command from SPANNING TREE mode.

Example

```
Dell(conf)#protocol spanning-tree 0
Dell(config-stp)#
```

Related Commands disable — disables spanning tree group 0. To enable spanning tree group 0, use the `no disable` command.

show config

Display the current configuration for the mode. Only non-default values display.

C9000 Series

Syntax `show config`

Command Modes SPANNING TREE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(config-stp)#show config
protocol spanning-tree 0
  no disable
Dell(config-stp)#
```

show spanning-tree 0

Display the spanning tree group configuration and status of interfaces in the spanning tree group.

C9000 Series

Syntax `show spanning-tree 0 [active | brief | guard | interface interface | root | summary]`

Parameters

0	Enter `0` (zero) to display information about that specific spanning tree group.
active	(OPTIONAL) Enter the keyword `active` to display only active interfaces in spanning tree group 0.
brief	(OPTIONAL) Enter the keyword `brief` to display a synopsis of the spanning tree group configuration information.
guard	(OPTIONAL) Enter the keyword `guard` to display the type of guard enabled on an STP interface and the current port state.
interface *interface*	(OPTIONAL) Enter the keyword `interface` and the type slot/port of the interface you want displayed. Type slot/port options are the following: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
root	(OPTIONAL) Enter the keyword `root` to display configuration information on the spanning tree group root.
summary	(OPTIONAL) Enter the keyword `summary` to only the number of ports in the spanning tree group and their state.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on the E-Series ExaScale.
8.4.2.1	Added support for the optional `guard` keyword on the C-Series, S-Series, and E-Series TeraScale.
8.3.7.0	Introduced on the S4810.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information Enable spanning tree group 0 prior to using this command.

The following describes the `show spanning-tree 0` command shown in the example.

Field	Description
"Bridge Identifier..."	Lists the bridge priority and the MAC address for this STP bridge.
"Configured hello..."	Displays the settings for hello time, max age, and forward delay.
"We are..."	States whether this bridge is the root bridge for the STG.
"Current root..."	Lists the bridge priority and MAC address for the root bridge.
"Topology flag..."	States whether the topology flag and the detected flag were set.
"Number of..."	Displays the number of topology changes, the time of the last topology change, and on what interface the topology change occurred.
"Timers"	Lists the values for the following bridge timers: hold time, topology change, hello time, max age, and forward delay.
"Times"	List the number of seconds since the last: • hello time • topology change • notification • aging
"Port 1..."	Displays the Interface type slot/port information and the status of the interface (Disabled or Enabled).
"Port path..."	Displays the path cost, priority, and identifier for the interface.

Field	Description
"Designated root..."	Displays the priority and MAC address of the root bridge of the STG that the interface belongs.
"Designated port..."	Displays the designated port ID.

The following describes the `show spanning-tree 0 guard` command shown in the Example (Guard).

Field	Description
Interface Name	STP interface.
Instance	STP 0 instance.
Sts	Port state: root-inconsistent (INCON Root), forwarding (FWD), listening (LIS), blocking (BLK), or shut down (EDS Shut).
Guard Type	Type of STP guard configured (Root, Loop, or BPDU guard).

The `peGigE` ports and VP-LAG ports information is displayed as part of the`show spanning-tree 0` command output, only when the `guard` option is entered.

Example

```
Dell#show spanning-tree 0

Executing IEEE compatible Spanning Tree Protocol
 Bridge Identifier has priority 32768, Address 0001.e800.0a56
 Configured hello time 2, max age 20, forward delay 15
 We are the root of the spanning tree
 Current root has priority 32768 address 0001.e800.0a56
 Topology change flag set, detected flag set
 Number of topology changes 1 last change occurred 0:00:05 ago
   from TenGigabitEthernet 1/3
 Timers:hold 1, topology change 35
        hello 2, max age 20, forward_delay 15
 Times:hello 1, topology change 1, notification 0, aging 2

Port 26 (TenGigabitEthernet 1/1) is Forwarding
 Port path cost 4, Port priority 8, Port Identifier 8.26
 Designated root has priority 32768, address 0001.e800.0a56
 Designated bridge has priority 32768, address 0001.e800.0a56
 Designated port id is 8.26, designated path cost 0
 Timers: message age 0, forward_delay 0, hold 0
 Number of transitions to forwarding state 1
 BPDU: sent:18, received 0
 The port is not in the portfast mode

Port 27 (TenGigabitEthernet 1/2) is Forwarding
 Port path cost 4, Port priority 8, Port Identifier 8.27
 Designated root has priority 32768, address 0001.e800.0a56
 Designated bridge has priority 32768, address 0001.e800.0a56
 Designated port id is 8.27, designated path cost 0
 Timers: message age 0, forward_delay 0, hold 0
 Number of transitions to forwarding state 1
 BPDU: sent:18, received 0
 The port is not in the portfast mode

Port 28 (TenGigabitEthernet 1/3) is Forwarding
 Port path cost 4, Port priority 8, Port Identifier 8.28
 Designated root has priority 32768, address 0001.e800.0a56
 Designated bridge has priority 32768, address 0001.e800.0a56
 Designated port id is 8.28, designated path cost 0
 Timers: message age 0, forward_delay 0, hold 0
 Number of transitions to forwarding state 1
 BPDU: sent:31, received 0
 The port is not in the portfast mode
```

```
Dell#
```

Example (Brief)

```
Dell#show span 0 brief
  Executing IEEE compatible Spanning Tree Protocol
    Root ID Priority 32768
      Address 0001.e800.0a56
    Root Bridge hello time 2, max age 20, forward delay 15
    Bridge ID Priority 32768,
      Address 0001.e800.0a56
    Configured hello time 2, max age 20, forward delay 15
Interface                          Designated
Name    PortID Prio Cost Sts Cost Bridge ID            PortID
--------------- ------ ---- ---- --- ----- ------------------
Te 1/1 8.26    8    4     FWD 0    32768 0001.e800.0a56 8.26
Te 1/2 8.27    8    4     FWD 0    32768 0001.e800.0a56 8.27
Te 1/3 8.28    8    4     FWD 0    32768 0001.e800.0a56 8.28
Dell#
```

Example (Guard)

```
Dell#show spanning-tree 0 guard
Interface
Name    Instance Sts          Guard type
--------- -------- --------- ----------
Te 0/1 0        INCON(Root)  Rootguard
Te 0/2 0        LIS          Loopguard
Te 0/3 0        EDS (Shut)   Bpduguard
```

spanning-tree 0

Assigns a Layer 2 interface to STP instance 0 and configures a port cost or port priority, or enables loop guard, root guard, or the Portfast feature on the interface.

C9000 Series

Syntax

`spanning-tree` *`stp-id`* `{cost` *`cost`* `| | portfast [bpduguard [shutdown-on-violation]] | priority` *`priority`*`}`

To disable Spanning Tree group on an interface, use the `no spanning-tree` *`stp-id`* `{cost` *`cost`* `| portfast [bpduguard [shutdown-on-violation]] | priority` *`priority`*`}` command.

Parameters

stp-id	Enter the STP instance ID. The range is 0.
cost *cost*	Enter the keyword `cost` then a number as the cost. The range is from 1 to 65535. The defaults are: • 10-Gigabit Ethernet interface = **2**. • Port Channel interface with 10-Gigabit Ethernet = **1**.
portfast [bpduguard [shutdown-on-violation]]	Enter the keyword `portfast` to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the optional keyword `bpduguard` to disable the port when it receives a BPDU.

Enter the optional keyword `shutdown-on-violation` to hardware disable an interface when a BPDU is received and the port is disabled.

priority *priority* — Enter keyword `priority` then a number as the priority. The range is from zero (0) to 15. The default is **8**.

Defaults cost = depends on the interface type; priority = **8**

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.1	Introduced the `loopguard` and `rootguard` options on the S4810.
8.4.2.1	Introduced the `loopguard` and `rootguard` options on the E-Series TeraScale, C-Series, and S-Series.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced the `shutdown-on-violation` option.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information If you enable `portfast bpduguard` on an interface and the interface receives a BPDU, the software disables the interface and sends a message stating that fact. The port is in ERR_DISABLE mode, yet appears in the `show interface` commands as enabled. If you do not enable `shutdown-on-violation`, BPDUs are still sent to the RPM CPU.

STP loop guard and root guard are supported on a port or port-channel enabled in any Spanning Tree mode: Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), Multiple Spanning Tree Protocol (MSTP), and Per-VLAN Spanning Tree Plus (PVST+).

Root guard is supported on any STP-enabled port or port-channel except when used as a stacking port. When enabled on a port, root guard applies to all VLANs configured on the port.

STP root guard and loop guard cannot be enabled at the same time on a port. For example, if you configure loop guard on a port on which root guard is already configured, the following error message is displayed: `% Error: RootGuard is configured. Cannot configure LoopGuard`.

Do not enable Portfast BPDU guard and loop guard at the same time on a port. Enabling both features may result in a port that remains in a blocking state and prevents traffic from flowing through it. For example, when Portfast BPDU guard and loop guard are both configured:

- If a BPDU is received from a remote device, BPDU guard places the port in an Err-Disabled Blocking state and no traffic is forwarded on the port.
- If no BPDU is received from a remote device, loop guard places the port in a Loop-Inconsistent Blocking state and no traffic is forwarded on the port.

To display the type of STP guard (Portfast BPDU, root, or loop guard) enabled on a port, enter the `show spanning-tree 0` command.

On PE ports and on VP-LAGs (lags formed with PE ports):

- spanning-tree with `bpdu guard shutdown-on-violation` is enabled by default.
- `no spanning tree` command is valid

Hence, you cannot issue the `spanning-tree` *`stp-id`* command on the PE ports (peGigE ports) and issuing this command on VP-LAG ports results in a failure.

59

Storm Control

The Dell Networking operating software storm control feature allows you to limit or suppress traffic during a traffic storm (Broadcast/ Unknown Unicast Rate Limiting or Multicast on the C-Series and S-Series).

Storm control is supported on Dell Networking OS.

Important Points to Remember

- Interface commands can only be applied on physical interfaces (virtual local area networks [VLANs] and link aggregation group [LAG] interfaces are not supported).
- An INTERFACE-level command only supports storm control configuration on ingress.
- An INTERFACE-level command overrides any CONFIGURATION-level ingress command for that physical interface, if both are configured.
- You can apply the CONFIGURATION-level storm control commands at ingress or egress and are supported on all physical interfaces.
- When storm control is applied on an interface, the percentage of storm control applied is calculated based on the advertised rate of the line card. It is not based on the speed setting for the line card.
- Do not apply per-VLAN quality of service (QoS) on an interface that has storm control enabled (either on an interface or globally).
- When you enable broadcast storm control on an interface or globally on ingress, and DSCP marking for a DSCP value 1 is configured for the data traffic, the traffic goes to queue 1 instead of queue 0.
- Similarly, if you enable unicast storm control on an interface or globally on ingress, and DSCP marking for a DSCP value 2 is configured for the data traffic, the traffic goes to queue 2 instead of queue 0.

NOTE: Bi-directional traffic (unknown unicast and broadcast) along with egress storm control causes the configured traffic rates split between the involved ports. The percentage of traffic that each port receives after the split is not predictable. These ports can be in the same/different port pipes or the same/different line cards.

NOTE: The policy discard drop counters are common across storm-control drops, ACL drops and QoS drops. Therefore, if your configuration includes ACL and QoS, those drops are also computed and displayed in the policy discard drops counter field along with storm-control drops. The packets dropped by the storm control feature can be monitored by viewing the value of the Policy Discard Drops field of the output of the `show hardware stack-unit stack-unit-number drops` command.

Topics:

- show storm-control broadcast
- show storm-control multicast
- show storm-control unknown-unicast
- storm-control broadcast (Configuration)
- storm-control broadcast (Interface)
- storm-control multicast (Configuration)
- storm-control multicast (Interface)
- storm-control pfc-llfc
- storm-control unknown-unicast (Configuration)
- storm-control unknown-unicast (Interface)

show storm-control broadcast

Display the storm control broadcast configuration.

C9000 Series

Syntax `show storm-control broadcast [interface]`

Parameters

interface (OPTIONAL) Enter one of the following interfaces to display the interface-specific storm control configuration:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

show storm-control multicast

Display the storm control multicast configuration.

C9000 Series

Syntax `show storm-control multicast [interface]`

Parameters

interface	(OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration: • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-Series and S-Series.

Example

```
Dell#show storm-control multicast tengigabitethernet 1/0

Multicast storm control configuration

Interface  Direction     Packets/Second
----------------------------------------
Te 1/0     Ingress       5
```

show storm-control unknown-unicast

Display the storm control unknown-unicast configuration.

C9000 Series

Syntax

```
show storm-control unknown-unicast [interface]
```

Parameters

interface (OPTIONAL) Enter one of the following interfaces to display the interface specific storm control configuration:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced on the E-Series.

storm-control broadcast (Configuration)

Configure the percentage of broadcast traffic allowed in the network.

C9000 Series

Syntax

`storm-control broadcast [packets_per_second in]`

To disable broadcast rate-limiting, use the `no storm-control broadcast [packets_per_second in]` command.

Parameters

packets_per_second in	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

Defaults

none

Command Modes

CONFIGURATION (conf)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added the `percentage decimal value` option.
6.5.1.0	Introduced on the E-Series.

Usage Information

Broadcast storm control is valid on Layer 2/Layer 3 interfaces only. Layer 2 broadcast traffic is treated as unknown-unicast traffic.

storm-control broadcast (Interface)

Configure the percentage of broadcast traffic allowed on an interface (ingress only).

C9000 Series

Syntax

`storm-control broadcast [packets_per_second in]`

To disable broadcast storm control on the interface, use the `no storm-control broadcast [packets_per_second in]` command.

Parameters

packets_per_second **in**	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

Defaults

none

Command Modes

INTERFACE (conf-if-*interface-slot/port*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added the `percentage decimal value` option.
6.5.1.0	Introduced on the E-Series.

storm-control multicast (Configuration)

Configure the packets per second (pps) of multicast traffic allowed into the C-Series and S-Series networks only.

C9000 Series

Syntax

`storm-control multicast packets_per_second in`

To disable storm-control for multicast traffic into the network, use the `no storm-control multicast packets_per_second in` command.

Parameters

packets_per_second in	Enter the packets per second of multicast traffic allowed into the network. The range is from 0 to 33554368.

Defaults none

Command Modes CONFIGURATION (conf)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-series and S-Series.

Usage Information Broadcast traffic (all 0xFs) should be counted against the broadcast storm control meter, not against the multicast storm control meter. It is possible, however, that some multicast control traffic may get dropped when storm control thresholds are exceeded.

storm-control multicast (Interface)

Configure the percentage of multicast traffic allowed on an C-Series or S-Series interface (ingress only) network only.

C9000 Series

Syntax `storm-control multicast packets_per_second in`

To disable multicast storm control on the interface, use the `no storm-control multicast packets_per_second in` command.

Parameters

packets_per_second in	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

Defaults none

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the C-series and S-Series.

storm-control pfc-llfc

Shut down a port if it receives more IEEE 802.1Qbb priority-based flow control (PFC) or IEEE 802.3X (Ethernet PAUSE) link-level flow control (LLFC) frames than the configured rate.

Syntax `storm-control pfc-llfc pps in shutdown`

Parameters

pfc-llfc *pps*	Enter a *pps* value to specify the threshold for flow-control traffic. The range is from 0 to 33554368 packets per second.
shutdown	Enter the keyword `shutdown` to shut down the port when flow-control traffic exceeds the configured rate.

Defaults None

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010, S4810, S4820T, S5000, S6000, Z9500, S3048-ON, S4048-ON, and S6000-ON.

Usage Information Use this command to disable a storm control-enabled interface when it receives continuous PFC/LLFC packets. This situation can occur if a faulty NIC or switch sends spurious PFC/LLFC packets.

storm-control unknown-unicast (Configuration)

Configure the percentage of unknown-unicast traffic allowed in or out of the network.

C9000 Series

Syntax `storm-control unknown-unicast [packets_per_second in]`

To disable storm control for unknown-unicast traffic, use the `no storm-control unknown-unicast [packets_per_second in]` command.

Parameters

packets_per_second in	Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554368.

Defaults none

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added the `percentage decimal value` option.
6.5.1.0	Introduced on the E-Series.

Usage Information Unknown Unicast Storm-Control is valid for Layer 2 and Layer 2/Layer 3 interfaces.

storm-control unknown-unicast (Interface)

Configure percentage of unknown-unicast traffic allowed on an interface (ingress only).

C9000 Series

Syntax `storm-control unknown-unicast [percentage decimal_value in] | [wred-profile name]] [packets_per_second in]`

To disable unknown-unicast storm control on the interface, use the `no storm-control unknown-unicast [percentage decimal_value in] | [wred-profile name]] [packets_per_second in]` command.

Parameters

percentage decimal_value [in | out]	E-Series Only: Enter the percentage of broadcast traffic allowed in or out of the network. Optionally, you can designate a decimal value percentage, for example, 55.5%. The percentage is from 0 to 100: • 0% blocks all related traffic. • 100% allows all traffic into the interface.

The decimal range is from 0.1 to 0.9.

wred-profile name	E-Series Only: (Optionally) Enter the keywords `wred-profile` followed by the profile name to designate a wred-profile.
***packets_per_second* in**	C-Series and S-Series Only: Enter the packets per second of broadcast traffic allowed into the network. The range is from 0 to 33554431.

Defaults none

Command Modes INTERFACE (conf-if-*interface-slot/port*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	E-Series Only: Added the `percentage decimal value` option.
6.5.1.0	Introduced on the E-Series.

60

SupportAssist

SupportAssist sends troubleshooting data securely to Dell. SupportAssist in this Dell Networking OS release does not support automated email notification at the time of hardware fault alert, automatic case creation, automatic part dispatch, or reports. SupportAssist requires Dell Networking OS 9.9(0.0) and SmartScripts 9.7 or later to be installed on the Dell Networking device. For more information on SmartScripts, see *Dell Networking Open Automation guide*.

NOTE: SupportAssist is enabled by default on the system. To disable SupportAssist, enter the `eula-consent support-assist reject` command in Global Configuration mode and save the configuration.

Topics:

- eula-consent
- support-assist
- support-assist activate
- support-assist activity
- SupportAssist Commands
- SupportAssist Activity Commands
- SupportAssist Company Commands
- SupportAssist Person Commands
- SupportAssist Server Commands
- show eula-consent
- show running-config
- show support-assist status

eula-consent

Accept or reject the end user license agreement (EULA).

Syntax `eula-consent {support-assist} {accept | reject}`

Parameters

support-assist	Enter the keywords `support-assist` to either accept or reject the EULA for the specified service.
accept	Enter the keyword `accept` to accept the EULA for the specified service.
reject	Enter the keyword `reject` to reject the EULA for the specified service.

Defaults None

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.

Version	Description
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

- When you run the command, the system displays a message with the information directing to the URL for further information.
- Even before you accept or reject the EULA, the configuration data is sent to the default centrally deployed SupportAssist Server. If you reject the EULA, the configuration data is not transmitted to the SupportAssist server.
- If there is an existing SupportAssist configuration, the configuration is not removed and the feature is disabled.

Example

Accept the EULA:

```
Dell(conf)# eula-consent support-assist accept
I accept the terms of the license agreement. You can reject
the license agreement by configuring this command
'eula-consent support-assist reject'.

By installing SupportAssist, you allow Dell to save your
contact information (e.g. name, phone number and/or
email address) which would be used to provide technical
support for your Dell products and services.  Dell may use
the information for providing recommendations to improve
your IT infrastructure.

Dell SupportAssist also collects and stores machine diagnostic
information, which may include but is not limited to
configuration information, user supplied contact information,
names of data volumes, IP addresses, access control lists,
diagnostics & performance information, network configuration
information, host/server configuration & performance
information and related data ("Collected Data") and transmits
this information to Dell. By downloading SupportAssist and
agreeing to be bound by these terms and the Dell end user
license agreement, available at: www.dell.com/aeula, you
agree to allow Dell to provide remote monitoring services of
your IT environment and you give Dell the right to collect the
Collected Data in accordance with Dells Privacy Policy,
available at: www.dell.com/privacypolicycountryspecific,
in order to enable the performance of all of the various
functions of SupportAssist during your entitlement to receive
related repair services from Dell,.  You further agree to
allow Dell to transmit and store the Collected Data from
SupportAssist in accordance with these terms.  You agree
that the provision of SupportAssist may involve international
transfers of data from you to Dell and/or to Dells affiliates,
subcontractors or business partners.  When making such
transfers, Dell shall ensure appropriate protection is in
place to safeguard the Collected Data being transferred in
connection with SupportAssist.  If you are downloading
SupportAssist on behalf of a company or other legal entity,
you are further certifying to Dell that you have
appropriate authority to provide this consent on behalf
of that entity.  If you do not consent to the collection,
transmission and/or use of the Collected Data, you may
not download, install or otherwise use SupportAssist.
```

Reject the EULA:

```
Dell(conf)#eula-consent support-assist reject
Aug 24 22:35:38: %STKUNIT1-M:CP %SUPPORT_ASSIST-6-SUPASSIST_EVT: Event monitor
service stopped
```

```
I do not accept the terms of the license agreement. The SupportAssist feature
has
been deactivated and can no longer be used.
To enable SupportAssist configurations, accept the terms of the license
agreement
by configuring this command 'eula-consent support-assist accept'.
Dell(conf)#
Dell(conf)#
Aug 24 22:35:49: %STKUNIT1-M:CP %SUPPORT_ASSIST-6-SUPASSIST_PKG_UNINSTALLED:
SupportAssist package uninstalled
Dell(conf)#
```

Related Commands

- support-assist — moves to the SupportAssist Configuration mode.

support-assist

Move to the SupportAssist configuration mode.

Syntax `support-assist`

To remove all the configuration of the SupportAssist service, use the `no support-assist` command.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information If you reject the EULA, the data is not transmitted to the SupportAssist server.

Related Commands

- eula-consent — accept or reject the EULA.

support-assist activate

Launch the configuration wizard that enables SupportAssist service and guides through a series of commands to configure SupportAssist.

Syntax `support-assist activate`

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.

Version	Description
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

You are guided through a series of queries to configure SupportAssist. The generated commands are added to the running configuration, including the DNS resolve commands, if configured.

This command starts the configuration wizard for the SupportAssist. At any time, you can exit by entering Ctrl-C. If necessary, you can skip some data entry.

Once you exit the wizard, the Dell Networking OS starts a full transfer.

support-assist activity

Trigger an activity event immediately.

Syntax

```
support-assist activity {full-transfer | core-transfer} start now
```

Parameters

full-transfer	Enter the keyword `full-transfer` to specify transfer of configuration, inventory, logs, and other information.
core-transfer	Enter the keyword `core-transfer` to specify transfer of core files.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

Use the command to trigger the activity that enables transfer of information. You can choose a full transfer that includes all the details or core transfer that includes only the core files.

NOTE: The full transfer includes the core files as well in the information sent. The core transfer does not send core files that are older than 30 days.

SupportAssist Commands

Dell Networking OS supports the following SupportAssist mode commands.

activity

Move to the SupportAssist Activity mode for an activity. Allow the user to configure customized details for a specific activity.

Syntax

`activity {activity-name}`

To remove all customized detail for a specific activity, use the `no activity {activity-name}` command.

Parameters

activity-name

Enter one of the following keywords:

- Enter the keyword `full-transfer` to enable or disable full transfer. You can create a custom file to transfer the outputs from a set of show commands. By default, the full transfer runs once in every 30 days.
- Enter the keyword `core-transfer` to enable or disable core transfer.
- Enter the keyword `event-transfer` to enable or disable event transfer. You can create a custom file to monitor a set of events.

Command Modes

SUPPORTASSIST

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM. Introduced the `core-transfer` and `event-transfer` parameters.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

By default, each activity follows a set of default actions using a default schedule. Using this command, you can customize the set of actions and disable a certain activity.

contact-company

Configure the contact information for the company.

Syntax

`contact-company name {company-name}[company-next-name] ... [company-next-name]`

To remove the contact company information, use the `no contact-company` command.

Parameters

company-name

Enter the name for the company. If there are multiple words in the name, use optional additional fields.

company-next-name

(OPTIONAL) Enter the next components of the company name, up to 5 components are allowed.

Command Modes SUPPORTASSIST

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information You can configure only one contact-company.

It is not possible to remove the components of the company name. The no form of the command removes the entire contact-company entry.

This command is optional for SupportAssist service configuration.

contact-person

Configure the contact name for an individual.

Syntax `contact-person [first <first-name>] last <last-name>`

To remove the contact person and all their details, use the `no contact-person [first <first-name>] last <last-name>` command.

Parameters

first-name	(Optional) Enter the first name for the contact person. This is optional provided each contact person name is unique. To include a space, enter a space within double quotes.
last-name	Enter the last name for the contact person. To include a space, enter a space within double quotes.

Command Modes SUPPORTASSIST

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information Each contact person must be unique by their name.

You can configure only one contact person.

It is not possible to remove the first name or last name. The no form of the command removes the entire contact-person entry.

This command is optional for SupportAssist service configuration.

enable

Enable all activities and severs for the SupportAssist service.

Syntax

```
enable all
```

To disable the SupportAssist activities temporarily, use the `no enable all` command.

Parameters

all	Enter the keyword `all` to enable all SupportAssist service activities.

Defaults

Enabled or All Enabled

Command Modes

SUPPORTASSIST

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

server

Configure the name of the remote SupportAssist Server and move to SupportAssist Server mode.

Syntax

```
server {default | server-name}
```

To delete a server, use the `no server server-name` command.

Parameters

default	Enter the keyword `default` for the default server.
server-name	Enter the name of the custom server to which the logs would be transferred. To include a space, enter a space within double quotes.

Defaults

Default server has URL stor.g3.ph.dell.com

Command Modes

SUPPORTASSIST

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.

Version	Description
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

The server-name is used as a reference only and is not required to be used as part of a URL definition.

There is a reserved name of `default` for the default server at stor.g3.ph.dell.com. You can customize the defaults for this server by entering the `server default` command and use the custom commands.

You can configure one additional server.

SupportAssist Activity Commands

Dell Networking OS supports the following SupportAssist Activity mode commands.

action-manifest get

Copy an action-manifest file for an activity to the system.

Syntax

```
action-manifest get tftp | ftp | flash <file-specification> <local-file-name>
```

Parameters

file-specification Enter the full file specification for the action-manifest file. For example:

- tftp://hostip/filepath
- ftp://userid:password@hostip/filepath
- scp://userid:password@hostip/filepath

local-file-name Enter the name of the local action-manifest file, up to 32 characters long. Allowable characters are: a to z, A to Z, 0 to 9, -, _, and space.

Command Modes

SUPPORTASSIST ACTIVITY FULL-TRANSFER

SUPPORTASSIST ACTIVITY EVENT-TRANSFER

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

The remote file specification for full transfer includes the protocol that is used to copy the file from the remote system.

The default Manifest-file for full transfer includes records like alarms, logs, operational, and configuration data.

Related Commands

- action-manifest install — configure the action-manifest to use for a specific activity.
- action-manifest show — view the list of action-manifest for a specific activity.
- action-manifest remove — remove the action-manifest file for an activity.

action-manifest install

Configure action-manifest to transfer a set of customized records for full transfer and to monitor a set of specified events for event transfer.

Syntax

`action-manifest install {default | <local-file-name>}`

To revert to the default action-manifest file, use the `action-manifest install default` command.

Parameters

default	Enter the keyword `default` to revert back to the default set of actions for an activity.
local-file-name	Enter the name of the local action-manifest file. Allowable characters are: a to z, A to Z, 0 to 9, -, _, and space.

Defaults

Default

Command Modes

SUPPORTASSIST ACTIVITY FULL-TRANSFER

SUPPORTASSIST ACTIVITY EVENT-TRANSFER

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

To replace the default action-manifest with a customized one, copy the action-manifest file to the system using the `action-manifest get` command and then use the `action-manifest install` command. To revert to the default action-manifest file, use the `action-manifest install default` command.

Related Commands

- action-manifest get — copy an action-manifest file for an activity to the system.
- action-manifest show — view the list of action-manifest for a specific activity.
- action-manifest remove — remove the action-manifest file for an activity.

action-manifest remove

Remove the action-manifest file from Dell Networking OS.

Syntax

```
action-manifest remove <local-file-name>}
```

Parameters

local-file-name	Enter the name of the local action-manifest file. Allowable characters are: a to z, A to Z, 0 to 9, -, _, and space.

Command Modes

SUPPORTASSIST ACTIVITY FULL-TRANSFER

SUPPORTASSIST ACTIVITY EVENT-TRANSFER

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

To revert to the default action-manifest file, use the `action-manifest install` command. If necessary, you can then remove the custom action-manifest file.

Related Commands

- action-manifest get — copy an action-manifest file for an activity to the system.
- action-manifest install — configure the action-manifest to use for a specific activity.
- action-manifest show — view the list of action-manifest for a specific activity.

action-manifest show

View the list of action-manifest for a specific activity.

Syntax

```
action-manifest show {all}
```

Parameters

all	Enter the keyword `all` to view the entire list of action-manifests that are available for an activity.

Command Modes

SUPPORTASSIST ACTIVITY FULL-TRANSFER

SUPPORTASSIST ACTIVITY EVENT-TRANSFER

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Related Commands

- action-manifest get — copy an action-manifest file for an activity to the system.
- action-manifest install — configure the action-manifest to use for a specific activity.
- action-manifest remove — remove the action-manifest file for an activity.

enable

Enable a specific SupportAssist activity.

Syntax `enable`

To disable a particular SupportAssist activity, use the `no enable` command.

Defaults Enabled

Command Modes SUPPORTASSIST ACTIVITY FULL-TRANSFER

SUPPORTASSIST ACTIVITY CORE-TRANSFER

SUPPORTASSIST ACTIVITY EVENT-TRANSFER

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information Enter the specific SupportAssist activity mode and then enable it.

NOTE: By default, the full transfer includes the core files. When you disable the core transfer activity, the full transfer excludes the core files.

Related Commands

- activity — move user to the SupportAssist Activity mode for that activity.

SupportAssist Company Commands

Dell Networking OS supports the following SupportAssist Company mode commands.

address

Configure the address information for the company.

Syntax

`address [city company-city] [{province | region | state} name] [country company-country] [{postalcode | zipcode] company-code]`

To remove a portion of the company address information, use the `no address [city | province | region | state | country | postalcode | zipcode]` command. For example, to remove the city alone, use the `no address city` command.

To remove the complete company contact information, use the `no address` command.

Parameters

city *company-city*	(OPTIONAL) Enter the keyword `city` then the city or town for the company site. To include a space, enter a space within double quotes.
province | region | state *name*	(OPTIONAL) Enter the keyword `province`, `region` or `state` then the name of province, region or state for the company site. To include a space, enter a space within double quotes.
country *company-country*	(OPTIONAL) Enter the keyword `country` then the country for the company site. To include a space, enter a space within double quotes.
postalcode | zipcode *company-code*	(OPTIONAL) Enter the keyword `postalcode` or `zipcode` then the postal code or zip code for the company site, as one string with no spaces.

Command Modes

SUPPORTASSIST COMPANY

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

The optional parameters must be provided in the following order: `city state country postalcode`. If specified in a different order, the command returns an error as follows:

```
Dell(conf-supportassist-cmpy-test)# address city Minneapolis postalcode 55344
country USA state Minnesota
                                  ^
% Error: Invalid input at "^" marker.
```

This command is optional for SupportAssist service configuration.

Example

```
Dell(conf-supportassist-cmpy-test)# address city Minneapolis state Minnesota
country USA postalcode 55344
```

street-address

Configure the street address information for the company.

Syntax

`street-address {address1} [address2]…[address8]`

To remove the street address, use the `no street-address` command.

Parameters

address1	Enter the street address for the company.
address2..address8	(OPTIONAL) Enter the street address of the company site. Up to 8 fields are allowed.

Command Modes

SUPPORTASSIST COMPANY

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

This command is optional for SupportAssist service configuration.

territory

Configure the territory and set the coverage for the company site.

Syntax

`territory company-territory`

To remove the company territory information, use the `no territory` command.

Parameters

company-territory	Enter the territory name for the company. To include a space, enter a space within double quotes. Use three-letter country codes like USA, IND, FRA, GER and so on.

Command Modes

SUPPORTASSIST COMPANY

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

This command is optional for SupportAssist service configuration.

SupportAssist Person Commands

Dell Networking OS supports the following SupportAssist Person mode commands.

email-address

Configure the email addresses to reach the contact person.

Syntax

`email-address primary` *`email-address`* `[alternate` *`email-address`*`]`

To remove an email address, use the `no email-address` command. To remove the primary and the alternate email addresses, use the `no email-address primary` and `no email-address alternate` commands respectively.

Parameters

primary *email-address*	Enter the keyword `primary` then the primary email address for the person.
alternate *email-address*	Enter the keyword `alternate` then the alternate email address for the person.

Command Modes

SUPPORTASSIST PERSON

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information

The email addresses must have the standard form of <username>@<email system> to be considered valid.

This command is optional for SupportAssist service configuration.

Related Commands

- preferred-method — configure the preferred method for contacting the person.

phone

Configure phone numbers to reach the contact person.

Syntax

`phone primary` *`phone`* `[alternate` *`phone`*`]`

To remove a phone number, use the `no phone` command. To remove the primary and alternate phone numbers, use the `no phone primary` and `no phone alternate` commands respectively.

Parameters

primary *phone*	Enter the keyword `primary` then the primary phone number for the person.
alternate *phone*	Enter the keyword `alternate` then the alternate phone number for the person.

Command Modes SUPPORTASSIST PERSON

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information The phone numbers may contain country codes, area codes and extensions, if necessary. Allowable characters are 0 to 9, x, (,), - and +.

This command is optional for SupportAssist service configuration.

Related Commands

- preferred-method — configure the preferred method for contacting the person.

preferred-method

Configure the preferred method for contacting the person.

Syntax `preferred-method {email | no-contact | phone]`

Parameters

email	Enter the keyword `email` to specify email as preferred method.
no-contact	Enter the keywords `no-contact` to specify that there is no preferred method.
phone	Enter the keyword `phone` to specify phone as preferred method.

Defaults no-contact

Command Modes SUPPORTASSIST PERSON

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Related Commands

- email-address — configure email addresses to reach the contact person.

- phone — configure phone numbers to reach the contact person.

time-zone

Configure the time zone for contacting the person.

Syntax

`time-zone zone +-HH:MM[start-time HH:MM] [end-time HH:MM]`

To remove the time zone, use the `no time-zone [zone | start-time | end-time]` command.

Parameters

zone *+-HH:MM*	Enter the keyword `zone` then a time difference from GMT expressed as HH:MM. This number may be preceded by either a + or – sign.
start-time *HH:MM*	Enter the keywords `start-time` then a starting time expressed as HH:MM. Use the 24-hour clock format.
stop-time *HH:MM*	Enter the keywords `stop-time` then a stopping time expressed as HH:MM. Use the 24-hour clock format.

Command Modes SUPPORTASSIST PERSON

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information This command is optional for SupportAssist service configuration.

SupportAssist Server Commands

Dell Networking OS supports the following SupportAssist Server mode commands.

proxy-ip-address

Configure a proxy for reaching the SupportAssist remote server.

Syntax

`proxy-ip-address {ipv4-address | ipv6-address} port port-number [ username userid password [encryption-type] password ]`

To remove the proxy, use the `no proxy-ip-address` command.

Parameters

ipv4-address	Enter the IP address of the proxy server in a dotted decimal format (A.B.C.D).
ipv6-address	Enter the IPv6 address of the proxy server in the x:x:x:x::x format.

NOTE: The :: notation specifies successive hexadecimal fields of zeros.

NOTE: To use the IPv6 address, the Open Automation package should also support IPv6 communications. For this purpose, SupportAssist requires Dell Networking Open Automation 9.10(0.0) package or later.

port *port-number*	Enter the keyword `port` then the TCP/IP port number. The port number range is from 1024 to 65534.
username *userid*	(OPTIONAL) Enter the keyword `username` then the user ID used for the proxy server.
password	Enter the keyword `password` then the encryption-type or the user password.
encryption-type	(OPTIONAL) Enter an encryption type for the *password* you enter. • 0 directs the system to interpret the password as clear text. • 7 indicates that the password is encrypted using a DES hashing algorithm.
password	Enter a string up to 32 characters long.

Defaults encryption-type for the password is 0.

Command Modes SUPPORTASSIST SERVER

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information The passwords are stored encrypted in the running configuration.

enable

Enable communication with the SupportAssist server.

Syntax `enable`

To disable communication to a specific SupportAssist server, use the `no enable` command.

Defaults Enabled

Command Modes SUPPORTASSIST SERVER

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.

Version	Description
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Related Commands

- server — configure the name of the remote SupportAssist server.

url

Configure the URL to reach the SupportAssist remote server.

Syntax `url uniform-resource-locator`

To delete the URL for the server, use the `no url` command.

Parameters

uniform-resource-locator	Enter a text string for the URL using one of the following formats: • http://[username:password@]<hostip>:<portNum>/<filepath> • https://[username:password@]<hostip>:<portNum>/<filepath> **NOTE: The host IP for the server may be specified as an IPv4 address, an IPv6 address or as a DNS hostname. If using the DNS hostname, the DNS resolver will need to be configured and enabled.**

Command Modes SUPPORTASSIST SERVER

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Usage Information The URL should be formatted to follow the ISO format.

show eula-consent

Display the EULA for the feature.

Syntax `show eula-consent {support-assist | other feature}`

Parameters

support-assist | *other feature*	Enter the keywords `support-assist` or the text corresponding to other feature.

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Example

```
Dell# show eula-consent support-assist

SupportAssist EULA has been: Accepted

Additional information about the SupportAssist EULA is as follows:

By installing SupportAssist, you allow Dell to save your contact information
(e.g. name, phone number and/or email address) which would be used to provide
technical support for your Dell products and services.  Dell may use the
information
for providing recommendations to improve  your IT infrastructure.

Dell SupportAssist also collects and stores machine diagnostic information,
which
may include but is not limited to configuration information, user supplied
contact
information, names of data volumes, IP addresses, access control lists,
diagnostics &
performance information, network configuration information, host/server
configuration
& performance information and related data (Collected Data) and transmits this
information to Dell. By downloading SupportAssist and agreeing to be bound by
these
terms and the Dell end user license agreement, available at: www.dell.com/
aeula,
you agree to allow Dell to provide remote monitoring services of your IT
environment
and you give Dell the right to collect the Collected Data in accordance with
Dells
Privacy Policy, available at: www.dell.com/privacypolicycountryspecific, in
order to
enable the performance of all of the various functions of SupportAssist during
your
entitlement to receive related repair services from Dell,.  You further agree
to
allow Dell to transmit and store the Collected Data from SupportAssist in
accordance
with these terms.  You agree that the provision of SupportAssist may involve
international transfers of data from you to Dell and/or to Dells affiliates,
subcontractors or business partners.  When making such transfers, Dell shall
ensure
appropriate protection is in place to safeguard the Collected Data being
transferred
in connection with SupportAssist.  If you are downloading SupportAssist on
behalf
of a company or other legal entity, you are further certifying to Dell that you
have appropriate authority to provide this consent on behalf of that entity.
If you
do not consent to the collection, transmission and/or use of the Collected
Data,
you may not download, install or otherwise use SupportAssist.
Dell#
```

show running-config

Display the current configuration and changes from the default values.

Syntax `show running-config support-assist`

Parameters

support-assist	Enter the keyword `support-assist` to view the detailed configuration for the feature.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Example

```
Dell# show running-config support-assist
!
support-assist
enable all
!
activity event-transfer
  enable
  action-manifest install default
!
activity core-transfer
  enable
!
contact-company name Dell
  street-address F lane , Sector 30
  address city Brussels state HeadState country Belgium postalcode S328J3
!
contact-person first Fred last Nash
  email-address primary des@sed.com alternate sed@dol.com
  phone primary 123422 alternate 8395729
  preferred-method email
  time-zone zone +05:30 start-time 12:23 end-time 15:23
!
server Dell
  enable
  url http://1.1.1.1:1332
Dell#
```

show support-assist status

Display information on SupportAssist feature status including any activities, status of communication, last time communication sent, and so on.

Syntax `show support-assist status`

Command Modes EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

Version	Description
9.11(0.0)	Introduced on the M I/O Aggregator and FN IOM.
9.10(0.0)	Introduced on the C9010, Z9100–ON, S6100–ON, and S3100 series.
9.9(0.0)	Introduced on the S4810, S4820T, S3048–ON, S4048–ON, S5000, S6000, S6000–ON, Z9500, MXL.

Example

```
Dell#show support-assist status
SupportAssist Service: Installed
EULA: Accepted
Server: default
    Enabled: Yes
    URL: https://stor.g3.ph.dell.com
Server: Dell
    Enabled: Yes
    URL: http://1.1.1.1:1332
Service status: Enabled

Activity                 State    Last Start                Last Success
-----------------------  -------  ------------------------
------------------------
core-transfer            Success  Feb 15 2016 09:43:41 IST    Feb 15 2016
09:43:56 IST
event-transfer           Success  Feb 15 2016 09:47:43 IST    Feb 15 2016
09:48:21 IST
full-transfer            Success  Feb 15 2016 09:36:12 IST    Feb 15 2016
09:38:27 IST
Dell#
```

61

System Time and Date

The commands in this chapter configure time values on the system, either using the Dell Networking operating software, or the hardware, or using the network time protocol (NTP). With NTP, the switch can act only as a client to an NTP clock host.

For more information, refer to the "Network Time Protocol" section of the *Management* chapter in the *Dell Networking OS Configuration Guide*.

Topics:

- clock set
- clock summer-time date
- clock summer-time recurring
- clock timezone
- debug ntp
- ntp authenticate
- ntp authentication-key
- ntp control-key-passwd
- ntp broadcast client
- ntp disable
- ntp master <stratum>
- ntp offset-threshold
- ntp server
- ntp source
- ntp trusted-key
- show clock
- show ntp associations
- show ntp status
- show ntp vrf associations

clock set

Set the software clock in the switch.

C9000 Series

Syntax `clock set time month day year`

Parameters

time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
month	Enter the name of one of the 12 months, in English. You can enter the number of a day and change the order of the display to time day month year.

	day	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time month day year.
	year	Enter a four-digit number as the year. The range is from 1993 to 2035.

Defaults Not configured.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information You can change the order of the `month` and `day` parameters to enter the time and date as time day month year. You cannot delete the software clock.

The software clock runs only when the software is up. The clock restarts, based on the hardware clock, when the switch reboots.

Dell Networking recommends using an outside time source, such as NTP, to ensure accurate time on the switch.

Example

```
Dell#clock set 16:20:00 19 may 2001
Dell#
```

clock summer-time date

Set a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.

C9000 Series

Syntax `clock summer-time` *time-zone* `date` *start-month start-day start-year start-time end-month end-day end-year end-time* `[`*offset*`]`

To delete a daylight saving time zone configuration, use the `no clock summer-time` command.

Parameters

time-zone	Enter the three-letter name for the time zone. This name is displayed in the show clock output.
start-month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.

start-day	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
start-year	Enter a four-digit number as the year. The range is from 1993 to 2035.
start-time	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
end-day	Enter the number of the day. The range is from 1 to 31. You can enter the name of a month to change the order of the display to time day month year.
end-month	Enter the name of one of the 12 months in English. You can enter the name of a day to change the order of the display to time day month year.
end-time	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
end-year	Enter a four-digit number as the year. The range is from 1993 to 2035.
offset	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is from 1 to1440. The default is **60 minutes**.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Related Commands

- clock summer-time recurring — sets a date (and time zone) on which to convert the switch to daylight saving time each year.
- show clock — displays the current clock settings.

clock summer-time recurring

Set the software clock to convert to daylight saving time on a specific day each year.

C9000 Series

Syntax

`clock summer-time` *`time-zone`* `recurring [`*`start-week start-day start-month start-time end-week end-day end-month end-time`* `[`*`offset`*`]]`

To delete a daylight saving time zone configuration, use the `no clock summer-time` command.

Parameters

time-zone	Enter the three-letter name for the time zone. This name is displayed in the show clock output. You can enter up to eight characters.
start-week	(OPTIONAL) Enter one of the following as the week that daylight saving begins and then enter values for start-day through end-time: • `week-number`: Enter a number from 1 to 4 as the number of the week in the month to start daylight saving time. • `first`: Enter this keyword to start daylight saving time in the first week of the month. • `last`: Enter this keyword to start daylight saving time in the last week of the month.
start-day	Enter the name of the day that you want daylight saving time to begin. Use English three letter abbreviations; for example, Sun, Sat, Mon, and so on. The range is from Sun to Sat.
start-month	Enter the name of one of the 12 months in English.
start-time	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
end-week	Enter the one of the following as the week that daylight saving ends: • `week-number`: enter a number from 1 to 4 as the number of the week to end daylight saving time. • `first`: enter the keyword `first` to end daylight saving time in the first week of the month. • `last`: enter the keyword `last` to end daylight saving time in the last week of the month.
end-day	Enter the weekday name that you want daylight saving time to end. Enter the weekdays using the three letter abbreviations; for example Sun, Sat, Mon, and so on. The range is from Sun to Sat.
end-month	Enter the name of one of the 12 months in English.
end-time	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
offset	(OPTIONAL) Enter the number of minutes to add during the summer-time period. The range is from 1 to 1440. The default is **60 minutes**.

Defaults

Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Updated the `start-day` and `end-day` options to allow for using the three-letter abbreviation of the weekday name.
6.1.1.0	Introduced on the E-Series.

Related Commands

- clock summer-time date — sets a date (and time zone) on which to convert the switch to daylight saving time on a one-time basis.
- show clock — displays the current clock settings

clock timezone

Configure a timezone for the switch.

C9000 Series

Syntax `clock timezone` *`timezone-name offset`*

To delete a timezone configuration, use the `no clock timezone` command.

Parameters

timezone-name	Enter the name of the timezone. You cannot use spaces.
offset	Enter one of the following: • a number from 1 to 23 as the number of hours in addition to universal time coordinated (UTC) for the timezone. • a minus sign (-) then a number from 1 to 23 as the number of hours.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

Coordinated universal time (UTC) is the time standard based on the International Atomic Time standard, commonly known as Greenwich Mean time. When determining system time, include the differentiator between UTC and your local timezone. For example, San Jose, CA is the Pacific Timezone with a UTC offset of -8.

debug ntp

Display Network Time Protocol (NTP) transactions and protocol messages for troubleshooting.

Syntax

`debug ntp {level` *`level-number`*`}`

To disable debugging of NTP transactions, use the `no debug ntp {level` *`level-number`*`}` command.

Parameters

level Enter the keyword `level` then the level–number to display information about NTP logs. The log level range is from 1 to 6.

- 1 is the most important log level.
- 6 is the least important log level.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the C9010, FN–IOM, MIOA, MXL, S3048–ON, S4048–ON, S4048T-ON, S5048F-ON, S6000, S6000–ON, S6010-ON, S6100–ON, and Z9100–ON.

ntp authenticate

Enable authentication of NTP traffic between the switch and the NTP time serving hosts.

C9000 Series

Syntax

```
ntp authenticate
```

To disable NTP authentication, use the `no ntp authentication` command.

Defaults

Not enabled.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

You also must configure an authentication key for NTP traffic using the `ntp authentication-key` command.

Related Commands

ntp authentication-key — configures the authentication key for NTP traffic.

ntp trusted-key — configures a key to authenticate.

ntp authentication-key

Specify a key for authenticating the NTP server.

Syntax

```
ntp authentication-key key-number {md5 | sha1} {0 | 7} key
```

Parameters

key-number	Specify a number for the authentication key. The range is from 1 to 65534. This number must be the same as the `number` parameter configured in the `ntp trusted-key` command.
md5	Specify that the authentication key is encrypted using MD5 encryption algorithm.

sha1	Specify that the authentication key is encrypted using SHA1 encryption algorithm.
0	Specify that authentication key is entered in an unencrypted format (default).
7	Specify that the authentication key is entered in DES encrypted format.
key	Enter the authentication key in the previously specified format.

Defaults

NTP authentication is not configured by default. If you do not specify the option [`0` | `7`], **0** is selected by default.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(1.0)	Introduced the `sha1` option. Also, introduced on the S4810 and S4820T.
9.14(0.0)	The trusted-key range value is from 1 to 65534.
9.12(1.0)	Introduced on the S5048F–ON.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Added options [`0` | `7`] for entering the authentication key.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

After configuring the `ntp authentication-key` command, configure the `ntp trusted-key` command to complete NTP authentication.

Dell EMC Networking OS versions 8.2.1.0 and later use an encryption algorithm to store the authentication key that is different from previous Dell EMC Networking OS versions; beginning in version 8.2.1.0, Dell EMC Networking OS uses DES encryption to store the key in the startup-config when you enter the `ntp authentication-key` command. Therefore, if your system boots with a startup-configuration from an Dell EMC Networking OS versions prior to 8.2.1.0 in which you have configured `ntp authentication-key`, the system cannot correctly decrypt the key, and cannot authenticate NTP packets. In this case you must re-enter this command and save the running-config to the startup-config.

Related Commands

- ntp authenticate — enables NTP authentication.
- ntp trusted-key — configures a trusted key.

ntp control-key-passwd

Configure control key password for NTPQ authentication. NTP control key supports encrypted and unencrypted option.

Syntax

```
ntp control-key-passwd [encryption-type] password
```

To delete the control key, use the `no ntp control-key-passwd [encryption-type] password` command.

Parameters

encryption-type (OPTIONAL) Enter one of the following numbers:

- 0 (zero) directs the system to store the password as clear text. It is the default encryption type when using the password option.
- 7 (seven) indicates that a password is encrypted using a DES hashing algorithm. It specifies a hidden authentication data.
- WORD is the un-encrypted (cleartext) authentication data.

password Enter a string up to 32 characters as the password.

Defaults NTPQ

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	Introduced on the C9010, FN–IOM, MIOA, MXL, S3048–ON, S4048–ON, S4048T–ON, S5048F–ON, S6000, S6000–ON, S6010–ON, S6100–ON, and Z9100–ON.

Usage Information NTP control key is not configured by default. If the encryption–type (0 or 7) is not specified, then 0 is selected by default.

ntp broadcast client

Set up the interface to receive NTP broadcasts from an NTP server.

C9000 Series

Syntax

```
ntp broadcast client
```

To disable broadcast, use the `no ntp broadcast client` command.

Defaults Disabled.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ntp disable

Prevent an interface from receiving NTP packets.

C9000 Series

Syntax `ntp disable`

To re-enable NTP on an interface, use the `no ntp disable` command.

Defaults Disabled (that is, if you configure an NTP host, all interfaces receive NTP packets)

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.1.1.0	Introduced on the E-Series.

ntp master <stratum>

Configure the switch as NTP Server.

Syntax `ntp master <stratum>`

Parameters

ntp master*<stratum>*	Enter the `stratum number` to identify the NTP Server's hierarchy. The `stratum` range value is from 2 to 15 and the default value is 8.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.6(0.0)	Introduced on the S4810, S4820T, S5000, S6000, Z9000, and Z9500.
9.2(1.0)	Introduced on the Z9500.

ntp offset-threshold

Configure the threshold time interval before which the system generates an NTP audit log message if the time difference from the NTP server is greater than a threshold value (offset-threshold).

Syntax `ntp offset-threshold threshold-value`

To disable the threshold value, use the `no ntp offset-threshold` command.

Parameters

offset-threshold ***threshold-value***	(Optional) Enter the keyword `offset-threshold` and then the threshold value. The range is from 0 to 999.

Defaults Zero (0).

Command Modes CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S3038–ON, S4048-ON, S3100 Series, S4810P, S4820T, S5000, S6000, S6000–ON, S6100–ON, Z9500, and Z9100–ON.

Usage Information

The `ntp offset-threshold` command does not time synchronization.

Example

```
DellEMC(config)# ntp offset-threshold 4
```

ntp server

Configure an NTP time-serving host.

Syntax

```
ntp server[vrf vrf-name] {hostname | ipv4-address | ipv6-address} [key keyid]
[prefer] [version number] [minpoll] [maxpoll]
```

Parameters

vrf *vrf-name*	(Optional) Enter the keyword `vrf` and then the name of the VRF to configure an NTP time-serving host corresponding to that VRF.
ipv4-address | *ipv6-address*	Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) of NTP server.
hostname	Enter the host name of the server.
key *keyid*	(OPTIONAL) Enter the keyword `key` and a number as the NTP peer key. The range is from 1 to 65534.
prefer	(OPTIONAL) Enter the keyword `prefer` to indicate that this peer has priority over other servers.
version *number*	(OPTIONAL) Enter the keyword `version` and a number to correspond to the NTP version used on the server. The range is from 1 to 4.
minpoll *polling-interval*	(OPTIONAL) Enter the keyword `minpoll`then the polling-interval. The polling interval range is from 4 to 16.
maxpoll *polling-interval*	(OPTIONAL) Enter the keyword `maxpoll`then the polling-interval. The polling interval range is from 4 to 16.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	The trusted-key range value is increased from 1 to 65534. Also, introduced the `minpoll` and `maxpoll` polling interval options.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.6(0.0)	Added support for VRF.
9.4.(0.0)	Added support for VRF.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Added IPv6 support.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

You can configure multiple time-serving hosts. From these time-serving hosts, the Dell EMC Networking OS chooses one NTP host with which to synchronize. To determine which server is selected, use the `show ntp associations` command.

Because many polls to NTP hosts can affect network performance, Dell EMC Networking recommends limiting the number of hosts configured.

By default, the system performs a time synchronization if the time difference from the time source is greater than one second.

When the Dell EMC Networking OS NTP client receives inconsistent timestamp in the origin timestamp filed, it logs the syslog message. It is due to the older versions of NTPD server implementation. Upgrade the system to the latest NTPD package in the NTP server and the system logs the following NTP syslog message:

```
Dell EMC# May 30 13:27:46 %STKUNIT2-:CP %ntp-6-: receive: Unexpected origin
timestamp 0xdeb95bee.06ba346e does not match aorg 0000000000.00000000 from
server@10.16.151.117 xmt 0xdeb95bee.30907a87
```

In general, the packet denied services are dropped with no further action except incrementing the statistics counters. In certain cases, a more proactive response is required to cause the client to slow down the process. A special packet is created to serve this purpose, and it is called the kiss-o-Death (KoD) packet. When the Dell EMC Networking OS client receives KoD packets, it logs the following syslog message:

```
Dell EMC# May 27 14:32:13 %STKUNIT1-:CP %ntp-6-: receive: KoD packet from
300::2 has inconsistent xmt/org/rec timestamps.  Ignoring.
```

Related Commands

- show ntp associations—displays the NTP servers that are configured and their status.

ntp source

Specify an interface's IP address to be included in the NTP packets.

Syntax

```
ntp source interface
```

To delete the configuration, use the `no ntp source` command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.
- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For the Management interface, enter the keyword `ManagementEthernet` then slot/port information.
- For a port-channel interface, enter the keywords `port-channel` then the port-channel ID.
- For VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.13.0.0	Added support for configuring Management interface.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards.
7.6.1.0	Introduced on the S-Series.

Version	Description
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

ntp trusted-key

Set a key to authenticate the system to which NTP synchronizes.

Syntax

`ntp trusted-key number`

To delete the key, use the `no ntp trusted-key number` command.

Parameters

number	Enter a number as the trusted key ID. The range is from 1 to 65534.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.14(0.0)	The trusted-key range value is increased from 1 to 65534.
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The `number` parameter in the `ntp trusted-key` command must be the same number as the `number` parameter in the `ntp authentication-key` command. If you change the `ntp authentication-key` command, you must also change the `ntp trusted-key` command.

Related Commands

- ntp authentication-key—sets an authentication key for NTP.

- ntp authenticate—enables the NTP authentication parameters you set.

show clock

Display the current clock settings.

C9000 Series

Syntax

```
show clock [detail]
```

From a **PE console**, use `show clock`.

Parameters

detail	(OPTIONAL) Enter the keyword `detail` to view the source information of the clock.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010 and C1048P.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show clock
11:05:56.949 UTC Thu Oct 25 2001
Dell#
```

Example (PE Console)

```
Dell#show clock
13:24:32.298 UTC Tue Jul 7 2015
```

Example (Detail)

```
Dell#show clock detail
12:18:10.691 UTC Wed Jan 7 2009
Time source is RTC hardware
Summer time starts 02:00:00 UTC Sun Mar 8 2009
Summer time ends 02:00:00 ABC Sun Nov 1 2009
Dell#
```

Related Commands clock summer-time recurring— displays the time and date from the switch hardware clock.

show ntp associations

Display the NTP master and peers.

Syntax `show ntp associations`

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information The following describes the `show ntp associations` command shown in the Example below.

Field	Description
(none)	One or more of the following symbols could be displayed: • * means synchronized to this peer. • # means almost synchronized to this peer. • + means the peer was selected for possible synchronization. • - means the peer is a candidate for selection. • x means designated falsesticker by the intersection algorithm.

Field	Description
remote	Displays the remote IP address of the NTP peer.
ref clock	Displays the IP address of the remote peer's reference clock.
st	Displays the peer's stratum, that is, the number of hops away from the external time source. A 16 in this column means the NTP peer cannot reach the time source.
when	Displays the last time the switch received an NTP packet.
poll	Displays the polling interval (in seconds).
reach	Displays the reachability to the peer (in octal bitstream).
delay	Displays the time interval or delay for a packet to complete a round-trip to the NTP time source (in milliseconds).
offset	Displays the relative time of the NTP peer's clock to the switch clock (in milliseconds).
offset	Displays the relative time of the NTP peer's clock to the switch clock (in milliseconds).
disp	Displays the dispersion.
LOCAL(0)	Indicates that the local machine has synced with itself. Generally, only a NTP master syncs with itself. Synchronization of the local machine takes place to this peer.
.LOCL.	Indicates the reference clock of the NTP master.

Example (without `ntp master` configuration)

```
DellEMC# show ntp associations
   remote       vrf-Id     ref clock    st when poll reach   delay   offset  disp
==============================================================================
*10.16.151.117   0      45.127.112.2    3   8   16   17    1.383  362.704  0.008
* master (synced), # backup, + selected, - outlier, x falseticker
```

Example (with `ntp master` configuration)

```
Dell EMC#show ntp associations
   remote       vrf-Id     ref clock     st when poll reach   delay   offset    disp
==============================================================================
*LOCAL(0)        0      .LOCL.           7    6   16  377      0.000    0.000
0.002
 10.16.127.86    0      10.16.127.26     5    9   16    1     65.292  13829.9
0.002
 10.16.127.144   0      10.16.127.26     5    6   16    1      0.829  13795.2
0.002
 10.16.127.44    0      10.16.127.26     5    -   16    1      0.799  13791.5
0.002
* master (synced), # backup, + selected, - outlier, x falseticker
Dell EMC#
```

In the above example,

- `LOCAL(0)` indicates that the local machine synchronizes with itself.
- `.LOCL.` indicates reference clock of the NTP master.

Related Commands

- show ntp status — displays the current NTP status.

show ntp status

Display the current NTP status.

Syntax `show ntp status`

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell EMC Networking OS Command Line Reference Guide*.

Version	Description
9.10(0.1)	Introduced on the S6010-ON and S4048T-ON.
9.10(0.0)	Introduced on the S3148.
9.10(0.0)	Introduced on the S6100–ON.
9.8(2.0)	Introduced on the S3100 series.
9.8(1.0)	Introduced on the Z9100–ON.
9.8(0.0P5)	Introduced on the S4048-ON.
9.8(0.0P2)	Introduced on the S3048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.1.1.0	Introduced on the E-Series.

Usage Information

The following describes the `show ntp status` command shown in the Example below.

Field	Description
"Clock is..."	States whether or not the switch clock is synchronized, which NTP stratum the system is assigned and the IP address of the NTP peer.
"frequency is..."	Displays the frequency (in ppm), stability (in ppm) and precision (in Hertz) of the clock in this system.
"reference time is..."	Displays the reference time stamp.
"clock offset is..."	Displays the system offset to the synchronized peer and the time delay on the path to the NTP root clock.
"root dispersion is..."	Displays the root and path dispersion.
"peer mode is..."	State what NTP mode the switch is. This should be Client mode.

Example

```
DellEMC#> show ntp status
Clock is synchronized, stratum 4, reference is 10.16.151.117, vrf-id is 0
frequency is 0.000 ppm, stability is 0.000 ppm, precision is -18
reference time  dec0e68a.07b308ac [Wed, Apr  7    0  9:42:34.030 UTC] UTC
clock offset is 0.000000 msec, root delay is 152.003 msec
root dispersion is 1381.293 msec, peer dispersion is 937.690 sec
```

```
peer mode is client
DellEMC#
```

Related Commands

- show ntp associations — displays information on the NTP master and peer configurations.

show ntp vrf associations

Displays the NTP servers configured for the VRF instance <vrf-name>.

C9000 Series

Syntax

show ntp `[vrf] <vrf-name>` associations.

```
Dell#show ntp vrf ? management
Dell#show ntp vrf management ?
associations            NTP associations
```

Command Modes

EXEC

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.6(0.0)	Added support for VRF.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	Added IPv6 support.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

62

Tunneling Commands

Tunnel interfaces create a logical tunnel for IPv4 or IPv6 traffic. You can configure DCSP, hop-limits and flow-labels. To enable a tunnel interface, use the following commands.

Topics:

- ip unnumbered
- ipv6 unnumbered
- tunnel allow-remote
- tunnel destination
- tunnel dscp
- tunnel flow-label
- tunnel hop-limit
- tunnel keepalive
- tunnel-mode
- tunnel source

ip unnumbered

Configure a tunnel interface to operate without a unique IPv4 address and select the interface from which the tunnel borrows its address.

C9000 Series

Syntax

ip unnumbered *{interface-type interface-number}*

To set the tunnel back to default logical address use the **no ip unnumbered** command. If the tunnel was previously operational, the tunnel interface is operationally down unless you also configure the tunnel IPv6 address.

Parameters

interface-type interface-number	Enter the interface type, followed by a slot number.

Defaults

None

Command Modes

INTERFACE TUNNEL

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.

Version	Description
9.3(0.1)	Introduced on the S6000 and Z9000.
9.4(0.1)	Introduced on the S4810, S4820T, S6000 and Z9000.

Usage Information

The ip unnumbered command fails in two conditions:

- If the logical ip address is configured.
- If Tunnel mode is ipv6ip (where ip address over tunnel interface is not possible).

To ping the unnumbered tunnels, the logical address route information must be present at both the ends.

NOTE: The `ip unnumbered` command can specify an interface name that does not exist or does not have a configured IPv6 address. The tunnel interface is not changed to operationally up until the logical ip address is identified from one of the address family.

ipv6 unnumbered

Configure a tunnel interface to operate without a unique IPv6 address and select the interface from which the tunnel borrows its address.

C9000 Series

Syntax

ipv6 unnumbered *{interface-type interface-number}*

To set the tunnel back to default logical address use the **no ipv6 unnumbered** command. If the tunnel was previously operational, the tunnel interface is operationally down unless you also configure the tunnel IPv4 address.

Parameters

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

interface-type interface-number	Enter the interface type, followed by the type, slot and port information.

Defaults

None.

Command Modes

INTERFACE TUNNEL

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.1)	Introduced on the S6000 and Z9000.
9.4(0.0)	Introduced on the S4810, S4820T, S6000 and Z9000.

Usage Information

The ip unnumbered command fails in two conditions:

- If the logical ip address is configured.

- If Tunnel mode is ipv6ip (where ip address over tunnel interface is not possible).

To ping the unnumbered tunnels, the logical address route information must be present at both the ends.

NOTE: The `ipv6 unnumbered` command can specify an interface name that does not exist or does not have a configured IPv6 address. The tunnel interface is not changed to operationally up until the logical ip address is identified from one of the address family.

tunnel allow-remote

Configure an IPv4 or IPv6 address or prefix whose tunneled packets are accepted for decapsulation. If you do not configure allow-remote entries, tunneled packets from any remote peer address is accepted.

This feature is supported on Dell Networking OS.

C9000 Series

Syntax

tunnel allow-remote {*ip-address* | *ipv6-address*} [*mask*]

To delete a configured allow-remote entry use the **no** `tunnel allow-remote` command. Any specified address/mask values must match an existing entry for the delete to succeed. If the address and mask are not specified, this command deletes all allow-remote entries.

Parameters

ip-address	Enter the source IPv4 address in A.B.C.D format.
ipv6–address	Enter the source IPv6 address in X:X:X:X::X format.
mask	(OPTIONAL) Enter a network mask in /prefix format (/x) or A.B.C.D to match a range of remote addresses. The default mask is /32 for IPv4 addresses and /128 for IPv6 addresses, which match only the specified address.

Defaults

If you do not configure tunnel allow remote , all traffic which is destined to tunnel source address is decapsulated.

Command Modes

INTERFACE TUNNEL

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.1)	Introduced on the S6000 and Z9000.
9.4(0.0)	Introduced on the S4810, S4820T, S6000 and Z9000.

Usage Information

You can configure up to eight allow-remote entries on any multipoint receive-only tunnel.

This command fails if the address family entered does not match the outer header address family of the tunnel mode, tunnel source, or any other tunnel allow-remote.

If you configure any allow-remote , the tunnel source or tunnel mode commands fail if the outer header address family does not match that of the configured allow-remote.

tunnel destination

Set a destination endpoint for the tunnel.

C9000 Series

Syntax

`tunnel destination {ip-address | ipv6-address}`

To delete a tunnel destination address, use the `no tunnel destination {ip-address | ipv6-address}` command.

Parameters

ip-address	Enter the destination IPv4 address for the tunnel.
ipv6–address	Enter the destination IPv6 address for the tunnel.

Defaults

none

Command Modes

INTERFACE TUNNEL (conf-if-tu)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S4820T, S6000 and Z9000.

Usage Information

The tunnel interface is inoperable without a valid tunnel destination address for the configured Tunnel mode.

To establish a logical tunnel to the particular destination address, use the destination address of the outer tunnel header. If you configure a tunnel interface or source address, the tunnel destination must be compatible.

tunnel dscp

Configure the method to set the DSCP in the outer tunnel header.

C9000 Series

Syntax

`tunnel dscp {mapped | value}`

To use the default tunnel mapping behavior, use the `no tunnel dscp value` command.

Parameters

mapped	Enter the keyword `mapped` to map the original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.
value	Enter a value to set the DSCP value in the tunnel header. The range is from 0 to 63. The default value of **0** denotes mapping of original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

Defaults 0 (Mapped)

Command Modes INTERFACE TUNNEL (conf-if-tu)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.3(0.0)	Introduced on the S6000, S4810, S4820T, Z9000.

Usage Information This command configures the method used to set the high 6 bits (the differentiated services codepoint) of the IPv4 TOS or the IPv6 traffic class in the outer IP header.

A value of 0 copies original packet DSCP (IPv4)/Traffic Class (IPv6) to the tunnel header DSCP (IPv4)/Traffic Class (IPv6) depending on the mode of tunnel.

tunnel flow-label

Configure the method to set the IPv6 flow label value in the outer tunnel header.

C9000 Series

Syntax `tunnel flow-label value`

To return to the default value of 0, use the `no tunnel flow-label value` command.

Parameters

value	Enter a value to set the IPv6 flow label value in the tunnel header. The range is from 0 to 1048575. The default value is **0**.

Defaults **0** (Mapped original packet flow-label value to tunnel header flow-label value)

Command Modes INTERFACE TUNNEL (conf-if-tu)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S6000, S4810, S4820T, Z9000.

Usage Information This command is only valid for tunnel interfaces with an IPv6 outer header.

tunnel hop-limit

Configure the method to set the IPv4 time-to-live or the IPv6 hop limit value in the outer tunnel header.

C9000 Series

Syntax

`tunnel hop-limit value`

To restore the default tunnel hop-limit, use the `no tunnel hop-limit` command.

Parameters

value	Enter the hop limit (ipv6) or time-to-live (ipv4) value to include in the tunnel header. The range is from 0 to 255. The default is **64**.

Defaults **64** (Time-to-live for IPv4 outer tunnel header or hop limit for IPv6 outer tunnel header)

Command Modes INTERFACE TUNNEL (conf-if-tu)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S6000, S4810, S4820T, Z9000.

Usage Information A value of 0 copies the inner packet hop limit (ipv6) or time-to-live (ipv4) in the encapsulated packet to the tunnel header hop limit (ipv6) or time-to-live (ipv4) value.

tunnel keepalive

Configure the tunnel keepalive target, interval and attempts.

C9000 Series

Syntax

`tunnel keepalive {ip-address | ipv6-address}[interval {seconds}] [attempts {count | unlimited}]`

To disable the tunnel keepalive probes use the **no tunnel keepalive** command.

Parameters

ip-address ipv6 address	Enter the `IPv4 or IPv6 address` of the peer to which the keepalive probes will be sent.
interval seconds	Enter the keyword `interval` then the interval time, in seconds, after which the restart process to keepalive probe packets. The range is from 5 to 255. The default is 5.

	count	(OPTIONAL) Enter the keyword **count** to count packets processed by the filter. The range is from 3 to 10. The default is 3.
	unlimited	Enter the keyword **unlimited** to specify the unlimited number of keepalive probe packets.

Defaults Tunnel keepalive is disabled.

Command Modes INTERFACE TUNNEL

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S4810, S4820T, S6000 and Z9000.

Usage Information Enabling tunnel keepalive causes ICMP echo packets to be sent to the keepalive target. The ICMP echo will be sourced from the tunnel interface logical IPv4 or IPv6 address and will be tunnel encapsulated. The response will be accepted whether it returns tunnel encapsulated or not.

When configuring tunnel keepalive at both end points of a tunnel interface it is recommended to set the tunnel keepalive target to the logical IPv4 or IPv6 address of the far end tunnel peer, rather than to the tunnel destination. This reduces the chance of both ends of the tunnel staying in keepalive down state. If both ends get into a keepalive down state that does not clear in a few seconds, then performing shutdown - no shutdown sequence on one end should bring both ends back to up.

tunnel-mode

Enable a tunnel interface.

.

C9000 Series

Syntax `tunnel mode {ipip | ipv6 | ipv6ip}[decapsulate-any]`

To disable an active tunnel interface, use the **no tunnel** `mode` command.

Parameters

ipip	Enable tunnel in RFC 2003 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv4 tunnel.
ipv6	Enable tunnel in RFC 2473 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv6 tunnel.
ipv6ip	Enable tunnel in RFC 4213 mode and encapsulate IPv6 datagrams inside an IPv4 tunnel.
decapsulate-any	(Optional) Enable tunnel in multipoint receive-only mode.

Defaults There is no default tunnel mode.

Command Modes INTERFACE TUNNEL

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.1)	Introduced on the S6000 and Z9000.
9.4(0.0)	Added the decapsulate-any command.

Usage Information

To enable a tunnel interface, use this command. You must define a tunnel mode for the tunnel to function. If you previously defined the tunnel destination or source address, the tunnel mode must be compatible.

Including the decapsulate-any option causes the command to fail if any of the following tunnel transmit options are configured: tunnel destination, tunnel dscp, tunnel flow-label, tunnel hop-limit, or tunnel keepalive. Conversely, if you configure any tunnel allow-remote entries, the `tunnel—mode` command fails unless the decapsulate-any option is included.

Configuration of IPv6 commands over decapsulate-any tunnel causes an error.

tunnel source

Set a source address for the tunnel.

C9000 Series

Syntax

`tunnel source {`*`ip-address`* `|` *`ipv6-address`* `|` *`interface-type-number`* `| anylocal}`

To delete the current tunnel source address, use the `no tunnel source` command.

Parameters

ip-address	Enter the source IPv4 address in A.B.C.D format.
ipv6–address	Enter the source IPv6 address in X:X:X:X::X format.
interface-type-number	• For a port channel interface, enter the keywords `port-channel` then a number from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.
anylocal	Enter the `anylocal` command to allow the multipoint receive-only tunnel to decapsulate tunnel packets destined to any local ip address.

Defaults

none

Command Modes

INTERFACE TUNNEL (conf-if-tu)

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Added the tunnel source anylocal command.
9.2(0.0)	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information

Added an optional keyword **"anylocal"** to the tunnel source command. The anylocal argument can be used in place of the ip address or interface, but only with the multipoint receive-only mode tunnels. The tunnel source `anylocal` command allows the multipoint receive-only tunnel to decapsulate tunnel packets addressed to any IPv4 or IPv6 (depending on the tunnel mode) address configured on the switch that is operationally **Up**.

63

Uplink Failure Detection (UFD)

Uplink failure detection (UFD) provides detection of the loss of upstream connectivity and, if you use this with NIC teaming, automatic recovery from a failed link.

Topics:

- clear ufd-disable
- debug uplink-state-group
- description
- downstream
- downstream auto-recover
- downstream disable links
- enable
- show running-config uplink-state-group
- show uplink-state-group
- uplink-state-group
- upstream

clear ufd-disable

Re-enable one or more downstream interfaces on the switch/router that are in a UFD-Disabled Error state so that an interface can send and receive traffic.

C9000 Series

Syntax

```
clear ufd-disable {interface interface | uplink-state-group group-id}
```

Parameters

interface *interface*

Specify one or more downstream interfaces. For *interface*, enter one of the following interface types:

- 10 Gigabit Ethernet: `tengigabitethernet {slot/port |slot/ port-range}`
- 40 Gigabit Ethernet: `fortyGigE {slot/port |slot/ port-range}`
- Port channel: `port-channel {1-512 | port-channel-range}`

Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

uplink-state-group *group-id*

Re-enables all UFD-disabled downstream interfaces in the group. The valid group-id values are from 1 to 16.

Defaults A downstream interface in a UFD-disabled uplink-state group is also disabled and is in a UFD-Disabled Error state.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

debug uplink-state-group

Enable debug messages for events related to a specified uplink-state group or all groups.

C9000 Series

Syntax `debug uplink-state-group [group-id]`

To turn off debugging event messages, enter the `no debug uplink-state-group [group-id]` command.

Parameters

group-id	Enables debugging on the specified uplink-state group. The valid group-id values are from 1 to 16.

Defaults none

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Related Commands clear ufd-disable — re-enables downstream interfaces that are in a UFD-Disabled Error state.

description

Enter a text description of an uplink-state group.

C9000 Series

Syntax `description text`

Parameters

text	Text description of the uplink-state group. The maximum length is 80 alphanumeric characters.

Defaults none

Command Modes UPLINK-STATE-GROUP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Example

```
Dell(conf-uplink-state-group-16)# description test
Dell(conf-uplink-state-group-16)#
```

Related Commands uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

downstream

Assign a port or port-channel to the uplink-state group as a downstream interface.

C9000 Series

Syntax `downstream interface`

To delete a downstream interface, enter the `no downstream interface` command.

Parameters

interface — Enter one of the following interface types:

- 10-Gigabit Ethernet: `tengigabitethernet {slot/port |slot/port-range}`
- 40-Gigabit Ethernet: `fortyGigE {slot/port |slot/port-range}`
- Port channel: `port-channel {1-512 | port-channel-range}`

Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults

none

Command Modes

UPLINK-STATE-GROUP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Usage Information

You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Related Commands

- upstream — assigns a port or port-channel to the uplink-state group as an upstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

downstream auto-recover

Enable auto-recovery so that UFD-disabled downstream ports in an uplink-state group automatically come up when a disabled upstream port in the group comes back up.

C9000 Series

Syntax

`downstream auto-recover`

To disable auto-recovery on downstream links, use the `no downstream auto-recover` command.

Defaults

The auto-recovery of UFD-disabled downstream ports is enabled.

Command Modes

UPLINK-STATE-GROUP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

downstream disable links

Configure the number of downstream links in the uplink-state group that are disabled if one upstream link in an uplink-state group goes down.

C9000 Series

Syntax

`downstream disable links {`*`number`*` |all}`

To revert to the default setting, use the `no downstream disable links` command.

Parameters

number	Enter the number of downstream links to be brought down by UFD. The range is from 1 to 1024.

all	Brings down all downstream links in the group.

Defaults No downstream links are disabled when an upstream link in an uplink-state group goes down.

Command Modes UPLINK-STATE-GROUP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Usage Information A user-configurable number of downstream interfaces in an uplink-state group are put into a link-down state with an UFD-Disabled error message when one upstream interface in an uplink-state group goes down.

If all upstream interfaces in an uplink-state group go down, all downstream interfaces in the same uplink-state group are put into a link-down state.

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

enable

Enable uplink state group tracking for a specific UFD group.

C9000 Series

Syntax `enable`

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command.

Defaults Upstream-link tracking is automatically enabled in an uplink-state group.

Command Modes UPLINK-STATE-GROUP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Related Commands

- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

show running-config uplink-state-group

Display the current configuration of one or more uplink-state groups.

C9000 Series

Syntax `show running-config uplink-state-group [group-id]`

Parameters

group-id	Displays the current configuration of all uplink-state groups or a specified group. The valid group-id values are from 1 to 16.

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Example

```
Dell#show running-config uplink-state-group
!
no enable
uplink state track 1
downstream TengigabitEthernet 0/2,4,6,11-19
upstream TengigabitEthernet 0/48, 52
upstream PortChannel 1
!
uplink state track 2
```

```
downstream TengigabitEthernet 0/1,3,5,7-10
upstream TengigabitEthernet 0/56,60
```

Related Commands

- show uplink-state-group — displays the status information on a specified uplink-state group or all groups.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

show uplink-state-group

Display status information on a specified uplink-state group or all groups.

C9000 Series

Syntax

```
show uplink-state-group [group-id] [detail]
```

Parameters

group-id	Displays status information on a specified uplink-state group or all groups. The valid group-id values are from 1 to 16.
detail	Displays additional status information on the upstream and downstream interfaces in each group

Defaults

none

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Example

```
Dell# show uplink-state-group
Uplink State Group: 1 Status: Enabled, Up
Uplink State Group: 3 Status: Enabled, Up
Uplink State Group: 5 Status: Enabled, Down
Uplink State Group: 6 Status: Enabled, Up
Uplink State Group: 7 Status: Enabled, Up
Uplink State Group: 16 Status: Disabled, Up

Dell# show uplink-state-group 16
Uplink State Group: 16 Status: Disabled, Up

Dell#show uplink-state-group detail
(Up): Interface up (Dwn): Interface down (Dis): Interface disabled
```

```
Uplink State Group    : 1 Status: Enabled, Up
Upstream Interfaces   :
Downstream Interfaces :

Uplink State Group    : 3 Status: Enabled, Up
Upstream Interfaces   : Te 0/46(Up) Te 0/47(Up)
Downstream Interfaces : Te 1/0(Up) Te 1/1(Up) Te 1/3(Up) Te 1/5(Up) Te 1/6(Up)

Uplink State Group    : 5 Status: Enabled, Down
Upstream Interfaces   : Te 0/0(Dwn) Te 0/3(Dwn) Te 0/5(Dwn)
Downstream Interfaces : Te 1/2(Dis) Te 1/4(Dis) Te 1/11(Dis) Te 1/12(Dis) Te
1/13(Dis) Te 1/14(Dis) Te 1/15(Dis)


Uplink State Group    : 6 Status: Enabled, Up
Upstream Interfaces   :
Downstream Interfaces :

Uplink State Group    : 7 Status: Enabled, Up
Upstream Interfaces   :
Downstream Interfaces :

Uplink State Group    : 16 Status: Disabled, Up
Upstream Interfaces   : Te 0/41(Dwn) Po 8(Dwn)
Downstream Interfaces : Te 0/40(Dwn)
```

Related Commands

- show running-config uplink-state-group — displays the current configuration of one or more uplink-state groups.
- uplink-state-group — create an uplink-state group and enables the tracking of upstream links.

uplink-state-group

Create an uplink-state group and enable the tracking of upstream links on a switch/ router.

C9000 Series

Syntax

`uplink-state-group` *group-id*

To delete an uplink-state group, enter the `no uplink-state-group group-id` command.

Parameters

group-id	Enter the ID number of an uplink-state group. The range is from 1 to 16.

Defaults

none

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Usage Information

After you enter the command, to assign upstream and downstream interfaces to the group, enter Uplink-State-Group Configuration mode.

An uplink-state group is considered to be operationally up if at least one upstream interface in the group is in the Link-Up state.

An uplink-state group is considered to be operationally down if no upstream interfaces in the group are in the Link-Up state. No uplink-state tracking is performed when a group is disabled or in an operationally down state.

To disable upstream-link tracking without deleting the uplink-state group, use the `no enable` command in uplink-state-group configuration mode.

Example

```
Dell(conf)#uplink-state-group 16
Dell(conf-uplink-state-group-16)#Dec 3 00:46:45: %SYSTEM:CP %IFMGR-5-
ASTATE_UP: Changed uplink state group
Admin state to up: Group 16
```

Related Commands

- show running-config uplink-state-group — displays the current configuration of one or more uplink-state groups.
- show uplink-state-group — displays the status information on a specified uplink-state group or all groups.

upstream

Assign a port or port-channel to the uplink-state group as an upstream interface.

C9000 Series

Syntax

`upstream` *`interface`*

To delete an upstream interface, use the `no upstream interface` command.

Parameters

interface Enter one of the following interface types:

- 10-Gigabit Ethernet: `tengigabitethernet {`*`slot/port | slot/port-range`*`}`
- 40-Gigabit Ethernet: `fortyGigE {`*`slot/port | slot/port-range`*`}`
- Port channel: `port-channel {`*`1-512 | port-channel-range`*`}`

Where `port-range` and `port-channel-range` specify a range of ports separated by a dash (-) and/or individual ports/port channels in any order; for example: `tengigabitethernet 1/1-2,5,9,11-12 port-channel 1-3,5`. A comma is required to separate each port and port-range entry.

Defaults none

Command Modes UPLINK-STATE-GROUP

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.
8.4.2.3	Introduced on the S-Series S50.

Usage Information You can assign physical port or port-channel interfaces to an uplink-state group.

You can assign an interface to only one uplink-state group. Configure each interface assigned to an uplink-state group as either an upstream or downstream interface, but not both.

You can assign individual member ports of a port channel to the group. An uplink-state group can contain either the member ports of a port channel or the port channel itself, but not both.

Example

```
Dell(conf-uplink-state-group-16)# upstream tengigabitethernet 1/10-15
Dell(conf-uplink-state-group-16)#
```

Related Commands

- downstream — assigns a port or port-channel to the uplink-state group as a downstream interface.
- uplink-state-group — creates an uplink-state group and enables the tracking of upstream links.

64

Virtual Link Trunking (VLT)

Virtual link trunking (VLT) allows physical links between two chassis to appear as a single virtual link to the network core. VLT eliminates the requirement for Spanning Tree protocols by allowing link aggregation group (LAG) terminations on two separate distribution or core switches, and by supporting a loop-free topology.

VLT provides Layer 2 multipathing, creating redundancy through increased bandwidth and enabling multiple parallel paths between nodes and load-balancing traffic where alternative paths exist.

NOTE: When you launch the VLT link, the VLT peer-ship is not established if any of the following is TRUE:

- The VLT System-MAC configured on both the VLT peers do not match.
- The VLT Unit-Id configured on both the VLT peers are identical.
- The VLT System-MAC or Unit-Id is configured only on one of the VLT peers.
- The VLT domain ID is not the same on both peers.

If the VLT peer-ship is already established, changing the System-MAC or Unit-Id does not cause VLT peer-ship to go down.

Also, if the VLT peer-ship is already established and the VLT Unit-Id or System-MAC are configured on both peers, then changing the CLI configurations on the VLT Unit-Id or System-MAC is rejected.

When the VLT peer-ship is already established, you can remove the VLT Unit-Id or System-MAC configuration from either or both peers. However, removing configuration settings can cause the VLT ports to go down.

Topics:

- back-up destination
- clear vlt statistics
- delay-restore
- lacp ungroup member-independent
- multicast peer-routing timeout
- peer-link port-channel
- peer-routing
- peer-routing-timeout
- primary-priority
- show vlt brief
- show vlt backup-link
- show vlt counters
- show vlt detail
- show vlt inconsistency
- show vlt mismatch
- show vlt private-vlan
- show vlt role
- show vlt statistics
- system-mac
- unit-id
- vlt domain

- vlt-peer-lag port-channel
- VLT Proxy Gateway

back-up destination

Configure the IPv4 or IPv6 address of the management interface on the remote VLT peer to be used as the endpoint of the VLT backup link for sending out-of-band hello messages.

C9000 Series

Syntax `back-up destination {[ipv4-address] | [ipv6 ipv6-address] [interval seconds]}`

Parameters

ipv4–address	Enter the IPv4 address of the backup destination.
ipv6	Enter the keyword `ipv6` then an IPv6 address in the X:X:X:X::X format.
interval *seconds*	Enter the keyword `interval` to specify the time interval to send hello messages. The range is from 1 to 5 seconds. The default is 1 second.

Defaults **1 second**

Command Modes VLT DOMAIN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.2)	Added support for IPv6.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

clear vlt statistics

Clear the statistics on VLT operations.

C9000 Series

Syntax `clear vlt statistics [arp | domain | igmp-snoop | mac | multicast | ndp]`

Parameters

domain	Clear the VLT statistics for the domain.
multicast	Clear the VLT statistics for multicast.
mac	Clear the VLT statistics for the MAC address.
arp	Clear the VLT statistics for ARP.
igmp-snoop	Clear the VLT statistics for IGMP snooping.
ndp	Clear the VLT statistics for NDP.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.2)	Added `multicast` and `ndp` parameters.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example

```
Dell(conf-vlt-domain)#do clear vlt statistics
Sure want to Clear VLT Statistics  [confirm] yes
Dell(conf-vlt-domain)#
```

Related Commands show vlt statistics — displays statistics on VLT operations.

delay-restore

Configure the delay in bringing up VLT ports after reload or peer-link restoration between the VLT peer switches.

C9000 Series

Syntax `delay-restore`

Parameters

delay-restore	Enter the amount of time, in seconds, to delay bringing up the VLT ports after the VLT device is reloaded or after the peer-link is restored between VLT peer switches. The range from 1 to 1200. The default is **90 seconds**.

Defaults Not configured.

Command Modes VLT DOMAIN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S8420T.
8.3.12.0	Introduced on the S4810.

Usage Information To delay the system from bringing up the VLT port for a brief period to allow IGMP Snooping and Layer 3 routing protocols to converge, use the `delay-restore` parameter. Use this feature:

- after a VLT device is reloaded.
- after the time when active VLTi link failed and restored.

Related Commands show vlt statistics — displays statistics on VLT operations.

lacp ungroup member-independent

Enables bare metal provisioning (BMP) booting of a top of rack (ToR) device through VLT nodes

C9000 Series

Syntax

```
lacp ungroup member-independent {vlt | port-channel}
```

Parameters

port-channel	Force all LACP port-channel members to become switchports.
vlt	Force all VLT LACP members to become switchports.

Defaults

Not configured.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Added port-channel parameter on the S4810.
8.3.8.0	Introduced on the S4810.

Usage Information

LACP on the VLT ports (on a VLT switch or access device), which are members of the virtual link trunk, is not brought up until the VLT domain is recognized on the access device.

During BMP reload, the ToR device or the device connected to the VLT port-channel must reach the DHCP server with the boot and configuration images. During boot-up, only untagged DHCP requests are sent to the DHCP server to receive an offer. To ungroup the VLT and port-channel configurations, use the `no lacp ungroup member independent` command on a VLT port channel, depending on whether the port channel is VLT or non-VLT. The DHCP server must be configured to start in BMP mode. If switches are connected using LACP port-channels like the VLT peer and ToR, use the `port-channel` parameter on the ToR-side configuration to allow member ports of an ungrouped LACP port-channel to inherit VLAN membership of that port channel to ensure untagged packets that are sent by a VLT peer device reach the DHCP server located on the ToR.

Example

```
Dell(conf)#lacp ungroup member-independent ?
port-channel                  LACP port-channel members become switchports
vlt                                    All VLT LACP members become switchports
```

multicast peer-routing timeout

Configure the time for a VLT node to retain synced multicast routes or synced multicast outgoing interface (OIF) after a VLT peer node failure.

C9000 Series

Syntax

`multicast peer-routing timeout value`

To restore the default value, use the `no multicast peer-routing timeout` command.

Parameters

value	Enter the timeout value in seconds. The range is from 1 to 1200. The default is 150.

Command Modes

VLT DOMAIN (conf-vlt-domain)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
9.0.2.0	Introduced on the S6000.

peer-link port-channel

Configure the specified port channel as the chassis interconnect trunk between VLT peers in the domain.

C9000 Series

Syntax

`peer-link port-channel port-channel-number {peer-down-vlan vlan id}`

Parameters

port-channel-number	Enter the port-channel number that acts as the interconnect trunk.
peer-down-vlan *vlan id*	Enter the keyword `peer-down-vlan` then a VLAN ID to configure the VLAN that the VLT peer link uses when the VLT peer is down.

Defaults

Not configured.

Command Modes

VLT DOMAIN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Added support for the **peer-down-vlan** parameter.
8.3.8.0	Introduced on the S4810.

Usage Information

To configure the VLAN from where the VLT peer forwards packets received over the VLTi from an adjacent VLT peer that is down, use the **peer-down-vlan** parameter. When a VLT peer with bare metal provisioning (BMP) is booting up, it sends untagged DHCP discover packets to its peer over the VLTi. To ensure that the DHCP discover packets are forwarded to the VLAN that has the DHCP server, use this configuration.

peer-routing

Enable L3 VLT peer-routing. This command is applicable for both IPV6/ IPV4.

C9000 Series

Syntax

`peer-routing`

To disable L3 VLT peer-routing, use the `no peer-routing` command.

Defaults

Disabled.

Command Modes

VLT DOMAIN (conf-vlt-domain)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added the support for IPV6 / IPV4.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.

Version	Description
9.2(0.2)	ntroduced on the Z9000, S4810, and S4820T.

peer-routing-timeout

Configure the delay after which peer routing is disabled when the peer is unavailable. This command is applicable for both IPV6/ IPV4.

C9000 Series

Syntax `peer-routing-timeout value`

To restore the default value, use the `no peer-routing-timeout` command.

Parameters

value	Enter the timeout value in seconds. The range is from 1 to 65535. The default value is 0 (no timeout).

Command Modes VLT DOMAIN (conf-vlt-domain)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added the support for IPV6 / IPV4.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
9.0.2.0	Introduced on the S6000.

Usage Information When the timer expires, the software checks to see if the VLT peer is now available. If the VLT peer is not available, peer-routing is disabled on that peer.

primary-priority

Assign the priority for master election among VLT peers.

C9000 Series

Syntax `[no] primary-priority`

Parameters

value	To configure the primary role of a VLT peer in a VLT domain, enter a lower value than the priority value of the remote peer. The range is from 1 to 65535.

Default **32768**

Command Modes VLT DOMAIN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Usage Information After you configure a VLT domain on each peer switch and connect (cable) the two VLT peers on each side of the VLT interconnect, the system elects a primary and secondary VLT peer device. To configure the primary and secondary roles before the election process, use the `primary-priority` command. Enter a lower value on the primary peer and a higher value on the secondary peer.

If the primary peer fails, the secondary peer (with the higher priority) takes the primary role. If the primary peer (with the lower priority) later comes back online, it is assigned the secondary role (there is no preemption).

show vlt brief

Displays summarized status information about VLT domains currently configured on the switch.

C9000 Series

Syntax `show vlt brief`

Default Not configured.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Usage Information The version shown in the `show vlt brief` output command displays the VLT version number which is different from the Dell Networking OS version number. VLT version numbers are begin with odd numbers such as 3 or 5.

Example (Brief)

```
Dell(conf) #show vlt brief
 VLT Domain Brief
----------------------------

Domain ID:                                10
Role:                                        Primary
Role Priority:                           32768
ICL Link Status:                        Up
Heart Beat Status:                   Not Established
VLT Peer Status:                        Up
Version:                                      5 (1)
Local System MAC address:        00:01:e8:8b:14:3c
Remote System MAC address:        00:01:e8:8b:15:20
Remote Sytem Version:                5 (1)
Delay-Restore timer:                90 seconds
```

show vlt backup-link

Displays information on the backup link operation.

C9000 Series

Syntax `show vlt backup-link`

Default Not configured.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Example

```
Dell_VLTpeer1# show vlt backup-link

VLT Backup Link
-----------------
```

```
Destination:                  10.11.200.18
Peer HeartBeat status:        Up
HeartBeat Timer Interval:     1
HeartBeat Timeout:            3
UDP Port:                     34998
HeartBeat Messages Sent:      1026
HeartBeat Messages Received: 1025
```

show vlt counters

Displays the counter information.

C9000 Series

Syntax `show vlt counters [arp| igmp-snoop | interface | mac | ndp]`

Parameters

arp	Enter the keyword `arp` to display the ARP counter information for the VLT.
igmp-snoop	Enter the keywords `igmp-snoop` to display the igmp-snooping counter information for the VLT.
interface	Enter the keyword `interface` to display the interface counter information for the VLT.
mac	Enter the keyword `mac` to display the MAC address counter information for the VLT.
ndp	Enter the keyword `ndp` to display the VLT counter information for NDP.

Default Not configured.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Usage Information If you do not add a parameter such as `arp` or `mac`, the output displays all of the counters.

Example

```
Dell# show vlt counter
Total VLT counters
------------------------
L2 Total MAC-Address Count :
IGMP MRouter Vlans count :
```

```
IGMP Mcast Groups count :
ARP entries count :
```

Example (igmp-snoop)

```
Dell# show vlt counter igmp-snoop
Total IGMP VLT counters
----------------------
IGMP MRouter Vlans count : 1
IGMP Mcast Groups count  : 5
```

Example (igmp-snoop interface port-channel)

```
Dell#show vlt counter igmp-snoop interface port-channel 2
VLT Port-ID: 2 IGMP Counter
-----------------------
IGMP MRouter Vlans count : 0
IGMP Mcast Groups count  : 5

Dell# show vlt counter igmp-snoop interface port-channel 100
VLT Port-ID: 100 IGMP Counter
-----------------------
IGMP MRouter Vlans count : 1
IGMP Mcast Groups count  : 0
Ve
```

Example (NDP and Non-VLT ARP)

```
Dell#show vlt counters
Total VLT Counters
-------------------
L2 Total MAC-Address Count:             2
Total Arp Entries Learnt :              0
Total Arp Entries Synced :              0
Total Non-VLT Arp entries Learnt:       0
Total Non-VLT Arp Entries Synced        0
IGMP MRouter Vlans count :
IGMP Mcast Groups count :
Total VLT Ndp Entries Learnt :          2
Total VLT Ndp Entries Synced :          0
Total Non-VLT Ndp Entries Learnt :      0
Total Non-VLT Ndp Entries Synced :      0
```

show vlt detail

Displays detailed status information about VLT port-channels currently configured on the switch.

C9000 Series

Syntax `show vlt detail`

Default Not configured.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.

Version	Description
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Example

```
Dell#show vlt detail
Local LAG Id Peer LAG Id Local Status Peer Status Active VLANs
------------ ----------- ------------ ------------ -------------
10           10          UP           UP           100, 200, 300, 400,
```

show vlt inconsistency

Display run-time inconsistencies in the incoming interface (IIF) for spanned multicast routes.

C9000 Series

Syntax `show vlt inconsistency ip mroute`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
9.0.2.0	Introduced on the S6000.

Example

```
Dell#show vlt inconsistency ip mroute
Spanned Multicast Routing IIF Inconsistency

Multicast Route                 LocalIIF      PeerIIF
---------------                 ----------    ---------
(22.22.22.200, 225.1.1.2)        VLAN 5       VLAN 6
(*, 225.1.1.2)                   VLAN 15      te 0/5
Dell#
```

show vlt mismatch

Display mismatches in VLT parameters.

C9000 Series

Syntax `show vlt mismatch`

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

Version

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Introduced the support for Q-in-Q implementation over VLT on the S-Series and Z-Series.
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Introduced on the Z9000, S4810, and S4820T.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.

Example

```
Dell#show vlt mismatch
Domain
-------
Parameters      Local     Peer
----------      -----     -----
 Unit-ID         0          1

Vlan-config
------------
Vlan-ID      Local Mode     Peer Mode
-------      ----------     ---------

100             --              L3

Vlan IPV4 Multicast Status
--------------------------
  Vlan-ID       Local Status       Peer Status
  --------      ------------       -----------

   4094           Active              Inactive

Dell#
```

Example for Q-in-Q implementation over VLT

```
Dell#show vlt mismatch
Domain
------
Parameters        Local              Peer
----------        -----              ----
PB for stp        Enabled           Disabled

Vlan-type-config
----------------
Codes:: P - Primary, C - Community, I - Isolated, N - Normal vlan, M - Vlan-
stack

Vlan-ID        Local    Peer
-------        -----    ----

 100            N        M

Port-type-config
----------------
Codes:: p - PVLAN Promiscuous port, h - PVLAN Host port, t - PVLAN Trunk port,
        mt - Vlan-stack trunk port, mu - Vlan-stack access port, n - Normal
port

Vlt Lag         Local     Peer
-------         -----     ----
128             mt        mu

Vlan-stack protocol-type
------------------------

Local      Peer
-----      ----
0x4100      0x8100

VLT-VLAN config
---------------

Local Lag    Peer Lag   Local VLANs        Peer VLANs
---------    --------   -----------        ----------
 128           128         4094            100

Dell#
```

show vlt private-vlan

Display the private VLAN (PVLAN) associated with the VLT LAG for VLT peer nodes.

C9000 Series

Syntax `show vlt private-vlan`

Command Modes EXEC

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S6000.

Version	Description
9.3(0.0)	Introduced on the Z9000, S4810, and S4820T.

Usage Information

If you add an ICL or VLTi link as a member of a primary VLAN, the ICL becomes a part of the primary VLAN and its associated secondary VLANs, similar to the behavior for normal trunk ports. VLAN symmetry is not validated if you associate an ICL to a PVLAN. Similarly, if you dissociate an ICL from a PVLAN, although the PVLAN symmetry exists, ICL is removed from that PVLAN in such a case. The **ICL Status** field denotes the type of the VLAN port of the VLTi link configured in a PVLAN.

Example

```
Dell#show vlt private-vlan vlan-id

Codes: C- Community, I - Isolated, V - Internally tagged, T - tagged, * - VLT
Pvlan
Primary    Secondary    ICL Status
10                        V (*)
            20(C)         V
            30 (I)       V

40                          T
            50(C)         T
            60 (I)       T
```

show vlt role

Displays the VLT peer status, role of the local VLT switch, VLT system MAC address and system priority, and the MAC address and priority of the local VLT device.

C9000 Series

Syntax

```
show vlt role
```

Default

Not configured.

Command Modes

EXEC

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Example

```
Dell_VLTpeer1# show vlt role

VLT Role
----------
```

```
VLT Role:                       Primary
System MAC address:             00:01:e8:8a:df:bc
System Role Priority:           32768
Local System MAC address:       00:01:e8:8a:df:bc
Local System Role Priority:     32768

Dell_VLTpeer2# show vlt role

VLT Role
----------
VLT Role:                       Secondary
System MAC address:             00:01:e8:8a:df:bc
System Role Priority:           32768
Local System MAC address:       00:01:e8:8a:df:e6
Local System Role Priority:     32768
```

show vlt statistics

Displays statistics on VLT operations.

C9000 Series

Syntax `show vlt statistics [arp | domain | igmp-snoop | mac | multicast | ndp]`

Parameters

domain	Display the VLT statistics for the domain.
multicast	Display the VLT statistics for multicast.
mac	Display the VLT statistics for the MAC address.
arp	Display the VLT statistics for ARP.
igmp-snoop	Display the VLT statistics for IGMP snooping.
ndp	Display the VLT statistics for NDP.

Default Not configured.

Command Modes EXEC

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.2)	Added parameters `multicast` and `ndp`
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Added support in the output for ARP, MAC, and IGMP snooping.

Version	Description
8.3.8.0	Introduced on the S4810.

Related Commands clear vlt statistics — clears the statistics on VLT operations.

Example

NOTE: The following example shows the statistics for *all* of the VLT parameters. If you enter a specific keyword, such as `mac`, only the statistics for that VLT parameter displays.

```
Dell_VLTpeer1#show vlt statistics
VLT Statistics
----------------
HeartBeat Messages Sent:     930
HeartBeat Messages Received: 909
ICL Hello's Sent:            927
ICL Hello's Received:        910
Domain Mismatch Errors:      0
Version Mismatch Errors:     0
Config Mismatch Errors:      0

VLT MAC Statistics
----------------
L2 Info Pkts sent:6, L2 Mac-sync Pkts Sent:0
L2 Info Pkts Rcvd:3, L2 Mac-sync Pkts Rcvd:2
L2 Reg Request sent:1
L2 Reg Request rcvd:2
L2 Reg Response sent:1
L2 Reg Response rcvd:1

VLT Igmp-Snooping Statistics
------------------------------
IGMP Info Pkts sent:     4
IGMP Info Pkts Rcvd:     1
IGMP Reg Request sent:   1
IGMP Reg Request rcvd:   2
IGMP Reg Response sent:  1
IGMP Reg Response rcvd:  1
IGMP PDU Tunnel Pkt sent: 5
IGMP PDU Tunnel Pkt rcvd: 10
IGMP Tunnel PDUs sent:    10
IGMP Tunnel PDUs rcvd:    19

VLT Multicast Statistics
------------------------------
Info Pkts Sent:                  4
Info Pkts Rcvd:                  2
Reg Request Sent:                2
Reg Request Rcvd:                2
Reg Response Sent:               1
Reg Response Rcvd:               0
Route updates sent to Peer:      0
Route updates rcvd from Peer:   0
Route update pkts sent to Peer:  0
Route update pkts rcvd from Peer: 0

VLT NDP Statistics
--------------------
NDP NA VLT Tunnel Pkts sent:16
NDP NA VLT Tunnel Pkts Rcvd:46
NDP NA Non-VLT Tunnel Pkts sent:0
NDP NA Non-VLT  Tunnel Pkts Rcvd:0
Ndp-sync Pkts Sent:144
Ndp-sync Pkts Rcvd:105
Ndp Reg Request sent:25
Ndp Reg Request rcvd:24
```

system-mac

Configure the MAC address for use by VLT Port-channel LACP for the domain

C9000 Series

Syntax `system-mac mac-address`

Parameters

mac-address	Enter the system MAC address for the VLT domain.

Defaults Not configured.

Command Modes VLT DOMAIN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Usage Information When you create a VLT domain on a switch, Dell Networking OS automatically creates a VLT-system MAC address used for internal system operations.

To reconfigure the default MAC address for the domain by entering a new MAC address in the format nn:nn:nn:nn:nn:nn, use the `system-mac` command.

You must also reconfigure the same MAC address on the VLT peer switch.

unit-id

Explicitly configure the default unit ID of a VLT peer switch.

C9000 Series

Syntax `unit-id [0 | 1]`

Parameters

0 | 1	Configure the default unit ID of a VLT peer switch. Enter `0` for the first peer or enter `1` for the second peer.

Defaults Automatically assigned based on the MAC address of each VLT peer. The peer with the lower MAC address is assigned unit 0; the peer with the higher MAC address is assigned unit 1.

Command Modes VLT DOMAIN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Usage Information When you create a VLT domain on a switch, Dell Networking OS automatically assigns a unique unit ID (0 or 1) to each peer switch. The unit IDs are used for internal system operations. Use the `unit-id` command to explicitly configure the unit ID of a VLT peer. Configure a different unit ID (0 or 1) on each peer switch.

To minimize the time required for the VLT system to determine the unit ID assigned to each peer switch when one peer reboots, use this command.

vlt domain

Enable VLT on a switch, configure a VLT domain, and enter VLT-domain configuration mode.

C9000 Series

Syntax `vlt domain` *`domain-id`*

Parameters

domain-id	Enter the Domain ID number. Configure the same domain ID on the peer switch. The range of domain IDs is from 1 to 1000.

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Usage Information The VLT domain ID must be the same between the two VLT devices. If the domain ID is not the same, a syslog message is generated and VLT does not launch.

Related Commands show vlt — uses the `show vlt brief` command to display the delay-restore value.

vlt-peer-lag port-channel

Associate the port channel to the corresponding port channel in the VLT peer for the VLT connection to an attached device.

C9000 Series

Syntax `vlt-peer-lag port-channel` *id-number*

Parameters

id-number	Enter the respective vlt port-channel number of the peer device.

Defaults Not configured.

Command Modes INTERFACE PORT-CHANNEL

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

VLT Proxy Gateway

The Virtual link trucking (VLT) proxy gateway feature allows a VLT domain to locally terminate and route L3 packets that are destined to a L3 end point in another VLT domain. Enable the VLT proxy gateway using the link layer discover protocol (LLDP) method or the static configuration. For more information, refer to *Dell Networking OS Command Line Reference Guide*.

peer-domain-link port-channel exclude-vlan

Configure the VLT port channel, which is connected to remote VLT domain for Proxy Gateway and configure the VLANs that needs to be excluded from VLT Proxy Gateway.

C9000 Series

Syntax `[no] peer-domain-link port-channel interface-identifier exclude-vlan vlan-range`

Parameters

port-channel	Configure the proxy-gateway interface port-channel. Port channel range is from 1 to 128.
vlan-range	Enter the VLAN IDs in which proxy gateway is not needed. The VLANs are excluded from doing proxy gateway. The value can be a single VLAN ID or comma-separated, VLAN IDs or a range of VLAN IDs or a combination. For example: Comma-separated: 3, 4, 6 Range: 5-10 Combination: 3, 4, 5-10, 8

Command Modes VLT DOMAIN PROXY GW LLDP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information The VLT port channel interface which is connecting to the remote VLT domain must be configured as peer-domain-link. Configure the VLANs that needs to be excluded from VLT Proxy Gateway.

Example

```
Dell(conf)#vlt-domain 1
Dell(conf-vlt-domain)#proxy-gateway lldp
Dell(conf-vlt-domain-proxy-gw-lldp)#peer-domain-link port-channel 20 exclude-
vlan 3
```

proxy-gateway lldp

Enables the proxy-gateway feature using LLDP protocol.

C9000 Series

Syntax `[no] proxy-gateway lldp`

Command Modes VLT DOMAIN

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information The configuration is cached and sent to LLDP only in one of the following conditions:
1) The port-channel connecting the two VLT domains, across DC, must be a VLT LAG

2) The protocol lldp command is globally enabled

3) The proxy-gateway LLDP configuration is applied.

Example

```
Dell(conf)#vlt-domain 1
Dell(conf-vlt-domain#proxy-gateway lldp
```

proxy-gateway peer-timeout

Enable the VLT node to timeout the transmission of peer's mac address when the VLT peer is down.

C9000 Series

Syntax `[no] peer-timeout` *value*

Parameters

value	Enter the timeout value in seconds. The range is from 1 to 65535.

Command Modes VLT DOMAIN PROXY GW LLDP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.

Version	Description
9.7(0.0)	Removed the default value on the S-Series and Z-Series.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.

Usage Information In a square VLT topology with a single link connecting to the remote peers, If a VLT peer goes down, the local VLT node must be prompted to stop transmitting it's peer's MAC address. You can configure the `peer-timeout` *`value`* command to stop the local VLT node from transmitting the peer MAC address within the configured peer timeout value. The default timeout value is infinity. You must enable the `vlt-peer-mac transmit` to configure a peer time out value.

Example

```
Dell(conf-vlt-domain-proxy-gw-lldp)# peer-timeout 5
```

proxy-gateway static

Enable the proxy-gateway feature using static configurations.

C9000 Series

Syntax `[no] proxy-gateway static`

Command Modes VLT DOMAIN

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000.

Usage Information When proxy-gateway static configuration is added, the setting is saved in the Layer 2 module. When you remove the static proxy gateway configuration, each `proxy-gateway static` mac configured is deleted from the Layer 2 module.

Example

```
Dell(conf)#vlt-domain 1
Dell(conf-vlt-domain#proxy-gateway static
```

remote-mac-address exclude-vlan

Configure the proxy-gateway static entry and exclude a VLAN or a range of VLANs from proxy routing.

C9000 Series

Syntax `[no] remote-mac-address` *`mac—address`* `[exclude-vlan` *`vlan-range`*`]`

Parameters

remote-mac-address	Specify the mac-addresses of the VLT peers which are in the remote VLT Domain.

mac-address	Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
vlan-range	Enter the `VLAN IDs` in which proxy gateway is not needed. The VLANs are excluded from doing proxy gateway. The value can be a single VLAN ID or comma -separated, VLAN IDs or a range of VLAN IDs or a combination. For example: Comma-separated: 3, 4, 6 Range: 5-10 Combination: 3, 4, 5-10, 8

Command Modes VLT DOMAIN PROXY GW STATIC

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information You can configure the MAC address, of a VLT peer in remote VLT Domain, to be associated with the static VLT proxy gateway and exclude a VLAN or a range of VLANs from proxy routing..

Example

```
Dell(conf)#vlt-domain 1
Dell(conf-vlt-domain#proxy-gateway static
Dell(conf-vlt-domain-proxy-gw-static)#remote-mac-address 00:01:e8:06:95:ac
exclude-vlan 3
```

show vlt-proxy-gateway

Display the VLT proxy gateway configuration.

C9000 Series

Syntax

```
show vlt-proxy-gateway [info] {lldp | static}
```

Parameters

lldp	Display details about the LLDP VLT proxy gateway configuration
static	Display details about the static VLT proxy gateway configuration

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information

At any point of time the proxy-gateway feature may go operationally down for the following reasons,

1) LLDP globally disabled

2) LLDP disabled per port

3) VLT port-channel is down

4) LLDP neighbor down

So, the proxy-gateway feature could be operationally down though properly configured and this will be reported in the “show command”.

When more than one VLT port-channel terminates on the same TOR, output of the `show VLT proxy-gateway info lldp` command may show the port-channel id incorrectly.

Example

```
Dell#show vlt proxy-gateway
 VLT Proxy Gateway Brief
-------------------------
 Config Mode:                          LLDP
 Global LLDP Config Status:            Enabled
 peer-mac-transmit Status:             Disabled

Dell#show vlt proxy-gateway info static
Mac Address           Exclude Vlan
-----------           ------------
00:01:e8:8a:e8:f7     3,7-8
00:01:e8:8b:1c:c0     3,7-8


Dell#show vlt proxy-gateway info lldp
LagId Mac Address     Exclude Vlan
----- -----------     ------------
Po 55 00:01:e8:8a:e8:f7 3,7-8 << Macs learnt via port-channel 55
Po 55 00:01:e8:8b:1c:c0 3,7-8
```

vlt-peer-mac transmit

Enable the device to transmit peer MAC address along with its own mac-address (in LLDP TLV packets) to the remote VLT Domain.

C9000 Series

Syntax `[no] vlt-peer-mac transmit`

Command Modes VLT DOMAIN PROXY GW LLDP

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON.
9.7(0.1)	Introduced on the S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5.(0.1)	Introduced on the Z9500
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information

This command enables the device to transmit its VLT peer's MAC address along with its own MAC address to the remote VLT domain. By default, a node sends only its own MAC address to the remote VLT domain. This configuration is applicable only for a LLDP proxy gateway.

Example

```
Dell(conf-vlt-domain-proxy-gw-lldp)# vlt-peer-mac transmit
```

65

Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is supported by the Dell Networking operating system.

Topics:

- IPv4 VRRP Commands
- IPv6 VRRP Commands

IPv4 VRRP Commands

The following are IPv4 VRRP commands.

advertise-interval

Set the time interval between VRRP advertisements.

C9000 Series

Syntax

`advertise-interval {`*`seconds`* `| centisecs` *`centisecs`* `}`

To return to the default settings, use the `no advertise-interval` command.

Parameters

seconds	Enter a number of seconds. The range is from 1 to 255. The default is **1 second**.
centisecs *centisecs*	Enter the keyword `centisecs` followed by the number of centisecs in multiple of 25 centisecs. The range is `25` to `4075` centisecs in multiples of `25` centisecs.

Defaults

1 second or 100 centisecs.

Command Modes

INTERFACE-VRRP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for centisecs on the Z9500.
9.5(0.0)	Added support for centisecs on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information Dell Networking recommends keeping the default setting for this command. If you do change the time interval between VRRP advertisements on one router, change it on all routers.

authentication-type

Enable authentication of VRRP data exchanges.

C9000 Series

Syntax `authentication-type simple [encryption-type] password`

To delete an authentication type and password, use the `no authentication-type` command.

Parameters

simple	Enter the keyword `simple` to specify simple authentication.
encryption-type	(OPTIONAL) Enter one of the following numbers: • `0` (zero) specifies an un-encrypted authentication data follows. • `7` (seven) specifies a hidden authentication data follows. • `LINE` is the un-encrypted (cleartext) authentication data.
password	Enter a character string up to eight characters long as a password. If you do not enter an encryption-type, the password is stored as clear text.

Defaults Not configured.

Command Modes VRRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

Version	Description
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information The given password is encrypted by the system and the `show config` displays an encrypted text string for any of the encrypted typed used.

clear counters vrrp

Clear the counters maintained on VRRP operations.

C9000 Series

Syntax `clear counters vrrp [vrrp-id] [ipv6][vrf vrf-name]`

Parameters

vrrp-id	(OPTIONAL) Enter the number of the VRRP group ID. The range is from 1 to 255.
ipv6	(OPTIONAL) Enter the keyword `ipv6` to clear counters from the IPv6 VRRP group.
vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to clear counters that are maintained on the VRRP operations corresponding to that VRF.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Added support for VRF.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell#clear counters vrrp vrf indus
Clear "show vrrp" counters of all vrrp groups on all interfaces in VRF indus
[confirm] yes
```

debug vrrp

Enable debugging of VRRP.

C9000 Series

Syntax

`debug vrrp` *`interface`* `[`*`vrrp-id`*`] {all | bfd | database | interface | ipv6 | packets | state | timer}`

To disable debugging, use the `no debug vrrp` *`interface`* `[`*`vrrp-id`*`] {all | bfd | database | interface | ipv6 | packets | state | timer}` command.

Parameters

interface	Enter the following keywords and slot/port or number information • For Port Channel interface types, enter the keywords `port-channel` then the number. The range is from 1 to 128. • For a 40-Gigabit Ethernet interface, enter the keyword `FortyGigabitEthernet` then the slot/port information. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
vrrp-id	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
all	Enter the keyword `all` to enable debugging of all VRRP groups.
bfd	Enter the keyword `bfd` to enable debugging of VRRP BFD interactions.
database	Enter the keyword `database` to enable debugging of configuration changes.
interface	Enter the keyword `interface` to enable debugging of interface state changes..
ipv6	Enter the keyword `ipv6` to enable debugging for IPv6.
packets	Enter the keyword `packets` to enable debugging of VRRP control packets.
state	Enter the keyword `state` to enable debugging of VRRP state changes.
timer	Enter the keyword `timer` to enable debugging of the VRRP timer.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information If no options are specified, debug is active on all interfaces and all VRRP groups.

description

Configure a short text string describing the VRRP group.

C9000 Series

Syntax `description text`

To delete a VRRP group description, use the `no description` command.

Parameters

text	Enter a text string up to 80 characters long.

Defaults Not enabled.

Command Modes VRRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

Version	Description
6.2.1.1	Introduced on the E-Series.

disable

Disable a VRRP group.

C9000 Series

Syntax `disable`

To re-enable a disabled VRRP group, use the `no disable` command.

Command Modes VRRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information To enable VRRP traffic, assign an IP address to the VRRP group using the `virtual-address` command and enter `no disable`.

Related Commands virtual-address — specifies the IP address of the virtual router.

hold-time

Specify a delay (in seconds) before a switch becomes the MASTER virtual router. By delaying the initialization of the VRRP MASTER, the new switch can stabilize its routing tables.

C9000 Series

Syntax `hold-time {`*`seconds`* `| centisecs` *`centisecs`*`}`

To return to the default value, use the `no hold-time` command.

Parameters

seconds	Enter the number of seconds. The range is from 0 to 65535. The default is **zero (0) seconds**.
centisecs *centisecs*	Enter the keyword `centisecs` then the number of *centisecs* in units of 25 centisecs . The range is from `0` to `65525` in units of 25 centisecs.

Defaults **zero (0) seconds or or (0) centiseconds**

Command Modes VRRP

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Added support for centisecs on the Z9500.
9.5(0.0)	Added support for centisecs on the Z9000, S6000, S4820T, S4810, and MXL.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information If a switch is a MASTER and you change the hold timer, disable and re-enable VRRP for the new hold timer value to take effect.

Related Commands disable — disables a VRRP group.

preempt

To preempt or become the MASTER router, permit a BACKUP router with a higher priority value.

C9000 Series

Syntax `preempt`

To prohibit preemption, use the `no preempt` command.

Defaults Enabled (that is, a BACKUP router can preempt the MASTER router).

Command Modes VRRP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

priority

Specify a VRRP priority value for the VRRP group. The VRRP protocol uses this value during the MASTER election process.

C9000 Series

Syntax

`priority` *priority*

To return to the default value, use the `no priority` command.

Parameters

priority	Enter a number as the priority. Enter 255 only if the router's virtual address is the same as the interface's primary IP address (that is, the router is the OWNER). The range is from 1 to 255. The default is **100**.

Defaults **100**

Command Modes VRRP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.16.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information

To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

If you set the `priority` command to 255 and the `virtual-address` is not equal to the interface's primary IP address, an error message appears.

show config

View the non-default VRRP configuration.

C9000 Series

Syntax

```
show config [verbose]
```

Parameters

verbose	(OPTIONAL) Enter the keyword `verbose` to view all VRRP group configuration information, including defaults.

Command Modes

VRRP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(conf-if-vrid-4)#show con
 vrrp-group 4
  virtual-address 119.192.182.124
 !
```

show vrrp

View the VRRP groups that are active. If no VRRP groups are active, the Dell Networking OS returns `No Active VRRP group`.

C9000 Series

Syntax `show vrrp [vrrp-id] [interface | brief | ipv6 | vrf vrf-name]`

Parameters

vrrp-id	(OPTIONAL) Enter the Virtual Router Identifier for the VRRP group to view only that group. The range is from 1 to 255.
interface	OPTIONAL) Enter the following keywords and slot/port or number information: • For Port Channel interface types, enter the keywords `port-channel` then the number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
brief	(OPTIONAL) Enter the keyword `brief` to view a table of information on the VRRP groups.
ipv6	(OPTIONAL) Enter the keyword `brief` to view a table of information on the VRRP groups.
vrf *vrf-name*	(OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to view active VRRP groups corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information The following describes the `show vrrp brief` command shown in the following example.

Item	Description
Interface	Lists the interface type, slot and port on which the VRRP group is configured.
Grp	Displays the VRRP group ID.
Pri	Displays the priority value assigned to the interface. If the `track` command is configured to track that interface and the interface is disabled, the cost is subtracted from the priority value assigned to the interface.
Pre	States whether preempt is enabled on the interface. • `Y` = Preempt is enabled. • `N` = Preempt is not enabled.
State	Displays the operational state of the interface by using one of the following: • NA/IF (the interface is not available). • MASTER (the interface associated with the MASTER router). • BACKUP (the interface associated with the BACKUP router).
Master addr	Displays the IP address of the MASTER router.
Virtual addr(s)	Displays the virtual IP addresses of the VRRP routers associated with the interface.

Usage Information The following describes the `show vrrp` command shown in the following example.

Field	Description
TenGigabitEthernet 12/3...	Displays the Interface, the VRRP group ID, and the network address. If the interface is not sending VRRP packets, 0.0.0.0 appears as the network address.
State: master...	Displays the interface's state: • Na/If (not available) • master (MASTER virtual router) • backup (BACKUP virtual router) the interface's priority and the IP address of the MASTER.
Hold Down:...	This line displays additional VRRP configuration information: • Hold Down displays the hold down timer interval in seconds. • Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured. • AdvInt displays the Advertise Interval in seconds.

Field	Description
Adv rcvd:...	This line displays counters for the following: • Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface. • Gratuitous ARP sent displays the number of gratuitous ARPs sent.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Authentication:...	States whether authentication is configured for the VRRP group. If it is, the authentication type and the password are listed.
Tracking states..	This line is displayed if the `track` command is configured on an interface. Below this line, the following information on the tracked interface is displayed: • Dn or Up states whether the interface is down or up. • the interface type slot/port information.

Example

```
Dell>show vrrp
------------------
TenGigabitEthernet 1/3, VRID: 1, Net: 10.1.1.253
State: Master, Priority: 105, Master: 10.1.1.253 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
  00:00:5e:00:01:01
Virtual IP address:
  10.1.1.252
Authentication: (none)
Tracking states for 1 interfaces:
  Up TenGigabitEthernet 1/17 priority-cost 10
------------------
TenGigabitEthernet 1/4, VRID: 2, Net: 10.1.2.253
State: Master, Priority: 110, Master: 10.1.2.253 (local)
Hold Down: 10 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Adv sent: 1862, Gratuitous ARP sent: 0
Virtual MAC address:
  00:00:5e:00:01:02
Virtual IP address:
  10.1.2.252
Authentication: (none)
Tracking states for 2 interfaces:
  Up TenGigabitEthernet 2/1 priority-cost 10
  Up TenGigabitEthernet 1/17 priority-cost 10
Dell>
```

Example (Brief)

```
Dell>Interface Grp Pri Pre State Master addr Virtual addr(s)
Description
-----------------------------------------------------
Te 1/37 1 100 Y Master 200.200.200.200 200.200.200.201
Te 1/37 2 100 Y Master 200.200.200.200 200.200.200.202 200.203 Description
Te 1/37 3 100 Y Master 1.1.1.1 1.1.1.2
Te 1/37 4 100 Y Master 200.200.200 200.200.200.206 200.200.207.. short desc
Te 1/37 254 254 Y Master 200.200.200.200 200.200.200.204 200.200.200.205
Dell>
```

Example (C9000)

```
Dell#show run vrf
!
ip vrf indus 1
Dell#show run int te 1/20
!
```

```
interface TenGigabitEthernet 1/20
ip vrf forwarding indus
ip address 2.1.1.1/24
!
vrrp-group 10
  authentication-type simple 7 7ba207e73007dfaf
  priority 200
  virtual-address 2.1.1.20
no shutdown
```

```
Dell#show vrrp vrf indus
------------------
TenGigabitEthernet 1/20, IPv4 VRID: 10, Version: 2, Net: 2.1.1.1
VRF: 1 indus
State: Master, Priority: 200, Master: 2.1.1.1 (local)
Hold Down: 0 sec, Preempt: TRUE, AdvInt: 1 sec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 107, Gratuitous ARP sent: 1
Virtual MAC address:
00:00:5e:00:01:0a
Virtual IP address:
2.1.1.20
Authentication:
type: simple
```

```
Dell#show vrrp vrf indus brief

Interface Group  Pri Pre State    Master addr     Virtual addr(s) Description
-------------------------------------------------------------------------------
Te 1/20          IPv4 10  200 Y   Master 2.1.1.1  2.1.1.20
Dell#
```

version

Set VRRP protocol version for IPv4 group.

C9000 Series

Syntax

`version {2 | 3 | both}`

To return to the default setting, use the `no version` command.

Parameters

2	Enter the `2` parameter to specify VRRP version 2 as defined by RFC 3768, *Virtual Router Redundancy Protocol*.
3	Enter the `2` parameter to specify VRRP version 3 as defined in RFC 5798, *Virtual Router Redundancy*.
both	Enter the `both` keyword for in-service migration from VRRP version 2 to VRRP version 3.

Defaults

2

Command Modes

VRRP

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.5(0.1)	Introduced on the Z9500.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Usage Information

You can use the version `both` command to migrate from VRRPv2 to VRRPv3. When you set the VRRP protocol version to both, the switch sends only VRRPv3 advertisements but can receive either VRRPv2 or VRRPv3 packets. To migrate an IPv4 VRRP group from VRRPv2 to VRRPv3:

1 Set the switches with the lowest priority to "both".

2 Set the switch with the highest priority to version to 3.

3 Set all the switches from both to version 3.

NOTE: Do not run VRRP version 2 and version 3 in the same group for an extended period of time.

Example

```
Dell(conf-if-te-0/0-vrid-100)#version ?
2                       VRRPv2
3                       VRRPv3
both                    Interoperable, send VRRPv3 receive
both

Dell(conf-if-te-0/0-vrid-100)#version 3
```

virtual-address

Configure up to 12 IP addresses of virtual routers in the VRRP group. To start sending VRRP packets, set at least one virtual address for the VRRP group.

C9000 Series

Syntax

`virtual-address` *ip-address1* `[...` *ip-address12*`]`

To delete one or more virtual IP addresses, use the `no virtual-address` *ip-address1* `[...` *ip-address12*`]` command.

Parameters

ip-address1	Enter an IP address of the virtual router in dotted decimal format. The IP address must be on the same subnet as the interface's primary IP address.
... ip-address12	(OPTIONAL) Enter up to 11 additional IP addresses of virtual routers in dotted decimal format. Separate the IP addresses with a space. The IP addresses must be on the same subnet as the interface's primary IP address.

Defaults

Not configured.

Command Modes

VRRP

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Introduced support for telnetting to the VRRP group IP address assigned using this command.
6.2.1.1	Introduced on the E-Series.

Usage Information

The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

A system message appears after you enter or delete the `virtual-address` command.

To guarantee that a VRRP group becomes MASTER, configure the VRRP group's virtual address with the same IP address as the interface's primary IP address and change the priority of the VRRP group to 255.

You can ping the virtual addresses configured in all VRRP groups.

vrrp delay minimum

Set the delay time for VRRP initialization after an interface comes up.

C9000 Series

Syntax `vrrp delay minimum seconds`

Parameters

seconds	Enter the number of seconds for the delay for VRRP initialization after an interface becomes operational. The range is from 0 to 900 (0 indicates no delay).

Defaults 0

Command Modes INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Usage Information This command applies to a single interface. When used with the `vrrp delay reload` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for VRRP.
- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

Related Command vrrp delay reload — sets the delay time for VRRP initialization after a system reboot.

vrrp delay reload

Set the delay time for VRRP initialization after a system reboot.

C9000 Series

Syntax `vrrp delay reload seconds`

Parameters

seconds	Enter the number of seconds for the delay. The range is from 0 to 900 (0 indicates no delay).

Defaults 0

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.8.0	Introduced on the S4810.

Usage Information This command applies to all the VRRP configured interfaces on a system. When used with the `vrrp delay minimum` CLI, the later timer rules the VRRP enabling. For example, if `vrrp delay reload` is 600 and the `vrrp delay minimum` is 300:

- When the system reloads, VRRP waits 600 seconds (10 minutes) to bring up VRRP on all interfaces that are up and configured for VRRP.

- When an interface comes up, whether as part of a system reload or an interface reload, the system waits 300 seconds (5 minutes) to bring up VRRP on that interface.

Save the configuration and reload the system for the delay timers to take effect.

Related Command vrrp delay minimum — sets the delay time for VRRP initialization after a line card reboot.

vrrp-group

Assign a VRRP ID to an interface. You can configure up to 255 VRRP groups per interface.

C9000 Series

Syntax `vrrp-group vrrp-id`

Parameters

vrrp-id	Enter a number as the group ID. The range is from 1 to 255.

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information The VRRP group only becomes active and sends VRRP packets when a virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

Related Command virtual-address — assigns up to 12 virtual IP addresses per VRRP group.

track

Monitor an interface and lower the priority value of the VRRP group on that interface if it is disabled.

C9000 Series

Syntax

`track` *interface* `[priority-cost` *cost*`]`

To disable monitoring, use the `no track interface` command.

Parameters

interface — OPTIONAL) Enter the following keywords and slot/port or number information:

- For a 1-Gigabit Ethernet interface, enter the keyword `GigabitEthernet` followed by the slot/port information.
- For a Loopback interface, enter the keyword `loopback` followed by a number from 0 to 16383.
- For a Port Channel interface, enter the keywords `port-channel` followed by the number. The range of port-channel IDs is 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` followed by the slot/port information.
- For SONET interfaces, enter the keyword `sonet` followed by the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `FortyGigE` followed by the slot/port information.
- For a tunnel interface, enter the keyword *tunnel* followed by the slot/port information.
- For a VLAN interface, enter the keyword `vlan` followed by the VLAN ID. The VLAN ID range is from 1 to 4094.
- For a port extender (PE) Gigabit Ethernet interface, enter the keyword `peGigE` followed by the *pe-id* /stack-unit *unit number / port-ID* number.
- For a port extender 10-Gigabit Ethernet interface, enter the keyword `peTenGigE` then the *pe-id / stack-unit / port-id* information. The *pe-id* range is from 0 to 255; the stack-unit *unit-number* range is from 0 to 7; and the *port-id* range is 25 to 28 or 49 to 52 depending on the PE.

priority-cost — (OPTIONAL) Enter a number as the amount to be subtracted from the priority value. The range is 1 to 254. The default is **10**.

Defaults priority cost = **10**

Command Modes VRRP

Command History

Version	Description
9.13.0.1P1	Introduced `peTenGigE` interface support on the C9010.
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.2.(1.0)	Introduced on the Z9500.

Version	Description
9.0.2.0	Introduced on the S6000.
7.6.1.0	Introduced on the S-Series (S50 only).
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

Usage Information If the interface is disabled, the cost value is subtracted from the priority value and forces a new MASTER election if the priority value is lower than the priority value in the BACKUP virtual routers.

IPv6 VRRP Commands

The following are IPv6 VRRP commands.

- clear counters vrrp ipv6
- debug vrrp ipv6
- show vrrp ipv6
- vrrp-ipv6-group

The following commands apply to IPv4 and IPv6:

- advertise-interval
- clear counters vrrp ipv6
- description
- disable
- hold-time
- preempt
- priority
- show config
- virtual-address

clear counters vrrp ipv6

Clear the counters recorded for IPv6 VRRP groups.

C9000 Series

Syntax `clear counters vrrp ipv6 [vrid | vrf instance]`

Parameters

vrid	(OPTIONAL) Enter the number of an IPv6 VRRP group. The range is from 1 to 255.
vrf *instance*	(OPTIONAL) Enter the name of a VRF instance (32 characters maximum) to clear the counters of all IPv6 VRRP groups in the specified VRF.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.4.1.0	Introduced on E-Series ExaScale, C-Series, and S-Series. Support was added for IPv6 VRRP groups in non-default VRF instances.
8.3.2.0	Introduced on the E-Series TeraScale.

debug vrrp ipv6

Enable debugging of VRRP.

C9000 Series

Syntax `debug vrrp ipv6 interface [vrid] {all | packets | state | timer}`

Parameters

interface	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
vrid	(OPTIONAL) Enter a number from 1 to 255 as the VRRP group ID.
all	Enter the keyword `all` to enable debugging of all VRRP groups.
bfd	Enter the keyword `bfd` to enable debugging of all VFFP BFD interactions.
database	Enter the keyword `database` to display changes related to group, prefix, and interface entries in the VRRP table.
packets	Enter the keyword `packets` to enable debugging of VRRP control packets.
state	Enter the keyword `state` to enable debugging of VRRP state changes
timer	Enter the keyword `timer` to enable debugging of the VRRP timer.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.4.1.0	Introduced on E-Series ExaScale, C-Series, and S-Series. Support was added for IPv6 VRRP groups in non-default VRF instances.
8.3.2.0	Introduced on the E-Series TeraScale.

Usage Information If no options are specified, debug is active on all interfaces and all VRRP groups.

show vrrp ipv6

View the IPv6 VRRP groups that are active. If no VRRP groups are active, the Dell Networking OS returns `No Active VRRP group`.

C9000 Series

Syntax `show vrrp ipv6 [vrid] [interface] [brief][vrf vrf-name]`

Parameters

vrid	(OPTIONAL) Enter the virtual router identifier for the VRRP group to view only that group. The range is from 1 to 255.
interface	Enter the following keywords and slot/port or number information: • For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information. • For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information. • For a VLAN interface, enter the keyword `vlan` then the VLAN ID. The VLAN ID range is from 1 to 4094.
brief	(OPTIONAL) Enter the keyword `brief` to view a table of information on the VRRP groups.
vrf *vrf-name*	Enter the keyword vrf followed by the name of the VRF to view IPv6 VRRP groups corresponding to that VRF.

Command Modes

- EXEC
- EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON. Added support for VRF.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.
8.3.2.0	Introduced on the E-Series TeraScale.

Usage Information The following describes the `show vrrp ipv6` command shown in the following example.

Line Beginning with	Description
GigabitEthernet...	Displays the Interface, the VRRP group ID, and the network address. If the interface is no sending VRRP packets, 0.0.0.0 appears as the network address.
VRF	VRF instance to which the interface (on which the VRRP group is configured) belongs.
State: master...	Displays the interface's state: • Na/If (not available). • master (MASTER virtual router). • backup (BACKUP virtual router). the interface's priority and the IP address of the MASTER.
Hold Down:...	This line displays additional VRRP configuration information: • Hold Down displays the hold down timer interval in seconds. • Preempt displays TRUE if preempt is configured and FALSE if preempt is not configured. • AdvInt displays the Advertise Interval in seconds.
Adv rcvd:...	This line displays counters for the following: • Adv rcvd displays the number of VRRP advertisements received on the interface. • Adv sent displays the number of VRRP advertisements sent on the interface. • Bad pkts rcvd displays the number of invalid packets received on the interface.
Virtual MAC address	Displays the virtual MAC address of the VRRP group.
Virtual IP address	Displays the virtual IP address of the VRRP router to which the interface is connected.
Tracking states...	Displays information on the tracked interfaces or objects configured for a VRRP group (`track` command), including: • UP or DOWN state of the tracked interface or object (Up or Dn). • Interface type and slot/port or object number, description, and time since the last change in the state of the tracked object.

Line Beginning with	Description
	• Cost subtracted from the VRRP group priority if the state of the tracked interface/ object goes DOWN.

Example

```
Dell#show vrrp ipv6
------------------
TenGigabitEthernet 5/6, IPv6 VRID: 255, Version: 3, Net:
fe80::201:e8ff:fe7a:6bb9
VRF: 0 default-vrf
State: Master, Priority: 101, Master: fe80::201:e8ff:fe7a:6bb9 (local)
Hold Down: 0 centisec, Preempt: TRUE, AdvInt: 100 centisec
Accept Mode: FALSE, Master AdvInt: 100 centisec
Adv rcvd: 0, Bad pkts rcvd: 0, Adv sent: 64
Virtual MAC address:
  00:00:5e:00:02:ff
Virtual IP address:
  1::255 fe80::255
```

vrrp-ipv6-group

Assign an interface to a VRRP group.

C9000 Series

Syntax `vrrp-ipv6-group vrid`

Parameters

vrid	Enter the virtual-router ID number of the VRRP group. The VRID range is from 1 to 255.

Defaults Not configured.

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2.(1.0)	Introduced on the Z9500.
8.4.2.1	The range of valid VRID values on the E-Series when VRF microcode is loaded in CAM changed from 1 to 15.
8.4.1.0	Introduced on the E-Series ExaScale, C-Series, and S-Series.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.2.0	Introduced on the E-Series TeraScale.

Usage Information

The VRRP group only becomes active and sends VRRP packets when a link-local virtual IP address is configured. When you delete the virtual address, the VRRP group stops sending VRRP packets.

NOTE: Configure the same VRID on neighboring routers (Dell Networking or non-Dell Networking) in the same VRRP group in order for all routers to interoperate.

Related Commands

virtual-address — assigns up to 12 virtual IP addresses per VRRP group.

Virtual Routing and Forwarding (VRF)

Virtual Routing and Forwarding (VRF) allows multiple instances of a routing table to co-exist on the same router at the same time.

ip unknown-unicast

Enable IPv4 catch-all route.

C9000 Series

Syntax

`ip unknown-unicast` [vrf *vrf-name*]

To remove the IPv4 catch-all route (0.0.0.0/0) from the LPM route forwarding table in hardware which gets added as a default configuration after the initialization of FIB Agent module, use the `no ip unknown-unicast` command.

Defaults

None

Parameters

vrf *vrf-name*	(Optional) Enter the keyword `vrf` followed by the name of the VRF to enable catch-all routes corresponding to that VRF.

Command Modes

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S–Series and Z9000.

Usage Information

Use this command to add the IPv4 catch-all route (0.0.0.0/0) in the LPM route forwarding table if it was deleted using the `no ip unknown-unicast` command previously. This will be the default configuration after reload.

ipv6 unknown-unicast

Disable soft forwarding of unknown IPv6 destination packets.

C9000 Series

Syntax

`[no] ipv6 unknown-unicast`

Defaults Soft forwarding is enabled.

Command Modes CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.7(0.1)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information All the default catch-all entries in the longest prefix match (LPM) table collect and transmit all unresolved IPv6 packets to the CPU, even if they are destined for unknown destinations.

description

Enter a descriptive name for a customer VRF.

C9000 Series

Syntax `description string`

To delete the descriptive name for a customer VRF, use the `no description string` command.

Parameters

string	Enter a descriptive name for the VRF.

Defaults None.

Command Modes VRF MODE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.4.(0.0)	Introduced on the S-Series.

Usage Information Use this command to specify a descriptive name for a VRF.

ip vrf forwarding

Attach an interface to a configured VRF.

C9000 Series

Syntax

`ip vrf forwarding {vrf-name | management}`

To delete an interface associated with a configured VRF, use the `no ip vrf forwarding {vrf-name | management}` command.

Parameters

vrf-name	Enter name of the VRF that you want to associate the interface to.
management	Use this keyword when you want to associate the interface to the management VRF.

Defaults

None (Interface is part of default VRF).

Command Modes

INTERFACE-CONFIG

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON and Z9500.
9.4.(0.0)	Introduced on the S-Series and Z9000.

Usage Information

Use this command to attach an interface to a configured VRF. You can attach an interface to either a non-default VRF or a management VRF. To assign a port-back to a default VRF, remove VRF association from the interface. You can use this only if there is no IP address configured on the interface.

There must be no prior Layer 3 configuration on the interface when configuring VRF.

VRF must be enabled prior to implementing this command.

You can configure an IP subnet or address on a physical or VLAN interface that overlaps the same IP subnet or address configured on another interface only if the interfaces are assigned to different VRFs. If two interfaces are assigned to the same VRF, you cannot configure overlapping IP subnets or the same IP address on them.

ip route-export

Enable route leaking between VRFs. Export or share IPv4 routes corresponding to one VRF with other non-default VRFs.

C9000 Series

Syntax `ip route-export tag [route-map-name]`

Parameters

route-export	Enter the `route-export` keyword to leak or share routes between VRFs.
tag	Enter a *tag* (export route target) to expose routes to other VRFs. This tag acts as an identifier for exported routes. You can use this identifier while importing these routes into another non-default VRF.
route-map-name	(Optional) Enter the name of the route-map to filter the exported routes. You can leak global routes for VRF. As the global RTM usually contains a large pool of routes, when the destination VRF imports global routes, these routes are duplicated into the VRF's RTM. As a result, it is mandatory to use route-maps to filter out leaked routes while sharing global routes with VRFs.

Defaults N/A

Command Modes VRF MODE
CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.

Usage Information Use the`ip route-export tag` command without specifying the route-map attribute to export all the routes corresponding to a source VRF. This action exposes source VRF routes to various other VRFs, which then import these routes using the `ip route-import tag` command. In Dell Networking OS, you can configure only one route-export per VRF as only one set of routes can be exposed for leaking (or sharing). However, you can configure multiple route-import targets because a VRF accepts routes from multiple VRFs.

You can expose a unique set of routes from the source VRF for sharing with other VRFs. When there are two VRFs export routes, there is no option to discretely filter leaked routes from each source VRF. You cannot import one set of routes from one VRF and another set of routes from another VRF.

Only active routes are eligible for sharing. For example, if one VRF has two routes corresponding to BGP and OSPF, and the BGP route is inactive, the OSPF route takes precedence over BGP. The inactive BGP route is not shared even when the target VRF has the filtering options enabled to match BGP.

Related Commands ip route-import – imports routes from another VRF.

ip route-import

Import IPv4 routes leaked by another VRF using the tag specified by that VRF during route-export process.

C9000 Series

Syntax `ip route-import tag [route-map–name]`

Parameters

route-import	Enter the keyword route-import to import routes into the VRF.
tag	Enter a tag (ASN number) to specify an import route target for importing routes from another VRF. To import leaked routes from another VRF, you must use the same ASN number that is specified as the export route target at the source VRF.
route-map-name	Enter the name of the route-map to filter the imported routes. **NOTE: You must use the route-map attribute while importing routes from the global RTM. Route-maps enable you to filter routes at the import end based on the matching criteria that you define in the route-map.**

Defaults Not configured.

Command Modes

- CONFIGURATION
- VRF MODE

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.

Usage Information You can configure multiple import conditions per VRF depending on the exporting VRF.

The export-target and import-target support only the match protocol and match prefix-list options, all other options configured in the route-map are ignored.

Related Commands ip route-export – exports routes to another VRF.

ipv6 route-export

Enable route leaking between VRFs. Export or share IPv6 routes corresponding to one VRF with other non-default VRFs.

C9000 Series

Syntax `ipv6 route-export tag [route-map-name]`

Parameters

route-export	Enter the keyword route-export to leak or share routes between VRFs.
tag	Enter a tag (ASN number) as the export route target to expose routes to other VRFs. This tag acts as an identifier for exported routes. You can use this identifier while importing these routes into another non-default VRF.
route-map-name	(Optional) Enter the name of the route-map to filter the exported routes. You can leak global routes to be made available to VRFs. As the global RTM usually contains a large pool of routes, when the destination VRF imports global routes, these routes will be duplicated into the VRF's RTM. As a result, it is mandatory to use route-maps to filter out leaked routes while sharing global routes with VRFs.

Defaults N/A

Command Modes VRF MODE

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introducued on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.

Usage Information You can use the `ip route-export tag` command without specifying the route-map attribute to export all the routes corresponding to a source VRF. This action exposes source VRF's routes to various other VRFs, which then import these routes using the `ip route-import tag` command. In Dell Networking OS, you can configure at most one route-export per VRF as only one set of routes is exposed for leaking. However, you can configure multiple route-import targets because a VRF accepts routes from multiple VRFs.

You can expose a unique set of routes from the source VRF for leaking to other VRFs. When two VRFs leak or export routes, there is no option to discretely filter leaked routes from each source VRF. You cannot import one set of routes from one VRF and another set of routes from another VRF.

Only active routes are eligible for leaking. For example, if one VRF has two routes corresponding to BGP and OSPF, in which the BGP route is not active, the OSPF route takes precedence over BGP. Even though the Target VRF has specified filtering options to match BGP, the BGP route is not leaked as that route is not active in the Source VRF.

Related Commands ipv6 route-import – imports IPv6 routes from another VRF.

ipv6 route-import

Import IPv6 routes leaked by another VRF using the tag specified by that VRF during export of these routes.

C9000 Series

Syntax `ipv6 route-import tag [route-map-name]`

Parameters

route-import	Enter the keyword route-import to import IPv6 routes into the VRF.

tag	Enter a tag (ASN number) to specify an import route target for importing routes from another VRF. To import leaked routes from another VRF, you must use the same ASN number that is specified as the export route target at the source VRF.
route-map-name	Enter the name of the route-map to filter the imported routes. **NOTE: You must use the route-map attribute while importing routes from the global RTM. Route-maps enable you to filter routes at the import end based on the matching criteria that you define in the route-map.**

Command Modes VRF MODE

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.

Usage Information It is possible to configure multiple import conditions per VRF depending on the exporting VRF.

The export-target and import-target support only the match protocol and match prefix-list options. Other options that are configured in the route-maps are ignored.

Related Commands ipv6 route-export – exports IPv6 routes to another VRF.

match source-protocol

Specify matching criteria while exporting or importing routes.

C9000 Series

Syntax
```
match source-protocol {bgp | isis | ospf | connected | static}
```

Parameters

bgp	Enter the keyword bgp to leak or share routes corresponding to the BGP protocol.
isis	Enter the keyword isis to leak or share routes corresponding to the ISIS protocol.
ospf	Enter the keyword ospf to leak or share routes corresponding to the OSPF protocol.
connected	Enter the keyword connected to leak or share connected routes corresponding to the VRF.
static	Enter the keyword static to leak or share static routes corresponding to the VRF.

Command Modes ROUTE MAP MODE

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.

Version	Description
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.

Usage Information

You can specify the matching criteria only after defining a route-map. Before using this command, you must enter the route map mode using the route-map route-map-name command. The match criteria that you specify is associated with the route-map that you define.

The export-target and import-target support only the match protocol and match prefix-list options. Other options that are configured in the route-maps are ignored.

Related Commands

ipv6 route-import – imports IPv6 routes from another VRF.

redistribute

Redistribute leaked or exported routes corresponding to specific protocols.

C9000 Series

Syntax

```
redistribute {imported-bgp | import-ospf | import-isis}
```

Parameters

imported-bgp	Enter the keyword imported-bgp to redistribute leaked routes that are learnt using the BGP protocol.
imported-ospf	Enter the keyword imported-ospf to redistribute leaked routes that are learnt using the OSPF protocol.
imported-isis	Enter the keyword imported-isis to redistribute leaked routes that are learnt using the ISIS protocol.
route-map	Enter the name of the route-map to specify the filtering criteria for imported routes.

Command Modes

CONFIGURATION

Command History

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000–ON, and Z9500.

Related Commands

ip route-import – imports routes from another VRF.

interface management

Associate a management port with a management VRF.

C9000 Series

Syntax

`interface management`

To delete the association between a management port and a management VRF, use the `no interface management` command.

Defaults

None.

Command Modes

VRF MODE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.
9.4.(0.0)	Introduced on the S-Series and Z9000.

Usage Information

Use this command to associate a management port with a management VRF. When you execute this command, the management ports corresponding to both the ACTIVE unit as well as the STANDBY unit are associated with the management VRF.

maximum dynamic-routes

Specify the maximum number of dynamic (protocol) routes a VRF can have.

C9000 Series

Syntax

`maximum dynamic-routes` *`limit`* {**warn-threshold** *`threshold-value`* | **warning-only**}

To remove the limit on the maximum number of routes used, use the `no maximum dynamic-routes` command.

Parameters

limit	Maximum number of routes allowed in a VRF. Valid range is from 1 to 16,000 (or maximum allowable for that platform if smaller value).

warning-threshold	Warning threshold value is expressed as a percentage of the limit value. When the number of routes reaches the specified percentage of the limit, a warning message is generated. Valid range is 1 to 100. When warn-threshold is used, once the limit is reached, additional dynamic routes will not be allowed.
warning-only	When the warning-only option is used, a syslog message will be thrown when maximum number of dynamic routes reaches the limit. Additional dynamic routes will still allowed.

Defaults No limit is set on the maximum number of dynamic routes for a VRF.

Command Modes CONFIGURATION-VRF

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OSCommand Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON and Z9500.
9.4(0.0)	Introduced on the S–Series.

Usage Information If the maximum route limit is not specified for a VRF, then it has unlimited space that extends to the maximum number of entries allowed for the system. This command is not applicable to the default and management VRFs.

show ip vrf

Display information corresponding to the VRFs that are configured in the system.

C9000 Series

Syntax `show ip [vrf vrf-name]`

Parameters

vrf *vrf-name*	Enter the keyword vrf and then the name of the VRF to display information corresponding to that VRF..

Command Modes EXEC

EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.

Version	Description
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S-Series and Z9000.

Example

```
Dell#show ip vrf
VRF-Name                            VRF-ID Interfaces

default                             0      Te 0/0-13,18-47,
                                           Fo 0/48,52,56,60,
                                           Ma 0/0,
                                           Ma 1/0,
                                           Ma 2/0,
                                           Ma 3/0,
                                           Ma 4/0,
                                           Ma 5/0,
                                           Ma 6/0,
                                           Ma 7/0,
                                           Ma 8/0,
                                           Ma 9/0,
                                           Ma 10/0,
                                           Ma 11/0,
Nu 0,
                                           Vl 1
test1                               1      Te 0/14,16-17
test2                               2      Te 0/15
management                          64



Dell#show ip vrf test1
VRF-Name                            VRF-ID Interfaces

test1                               1      Te 0/14,16-17
```

show run vrf

Displays configuration information corresponding to all the VRFs in the system.

C9000 Series

Syntax `show run vrf vrf-name`

Parameters

vrf *vrf-name*	Enter the keyword `vrf` and then the name of the VRF..

Command Modes

- EXEC
- EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.8(0.0)	Introduced on the S3048-ON and S4048-ON.
9.7(0.0)	Introduced on the S6000-ON and Z9500.
9.4.(0.0)	Introduced on the S-Series and Z9000.

Usage Information Use this command to display information from the running-config corresponding to either a specific VRF or all the VRFs in the system.

Example

```
Dell#show run vrf test3
!
ip vrf test3
 description "IT Department"
```

67

VLAN Stacking

With the virtual local area network (VLAN)-stacking feature (also called stackable VLANs and QinQ), you can "stack" VLANs into one tunnel and switch them through the network transparently.

For more information about basic VLAN commands, see the *Virtual LAN (VLAN) Commands* section in the Layer 2 chapter.

Important Points to Remember

- If you do not enable the spanning tree protocol (STP) across the stackable VLAN network, STP bridge protocol data units (BPDUs) from the customer's networks are tunneled across the stackable VLAN network.
- If you do enable STP across the stackable VLAN network, STP BPDUs from the customer's networks are consumed and not tunneled across the stackable VLAN network unless you enable protocol tunneling.

  NOTE: For more information about protocol tunneling on the E-Series, see Service Provider Bridging.
- Layer 3 protocols are not supported on a stackable VLAN network.
- Assigning an IP address to a stackable VLAN is supported when all the members are only stackable VLAN trunk ports. IP addresses on a stackable VLAN-enabled VLAN are not supported if the VLAN contains stackable VLAN access ports. This facility is provided for the simple network management protocol (SNMP) management over a stackable VLAN-enabled VLAN containing only stackable VLAN trunk interfaces. Layer 3 routing protocols on such a VLAN are not supported.
- Dell Networking recommends that you do not use the same MAC address, on different customer VLANs, on the same stackable VLAN.
- Interfaces configured using stackable VLAN access or stackable VLAN trunk commands do not switch traffic for the default VLAN. These interfaces are switch traffic only when they are added to a non-default VLAN.
- Starting with the Dell Networking OS version 7.8.1 for C-Series and S-Series (Dell Networking OS version 7.7.1 for E-Series, 8.2.1.0 for E-Series ExaScale), a vlan-stack trunk port is also allowed to be configured as a tagged port and as an untagged port for single-tagged VLANs. When the vlan-stack trunk port is also a member of an untagged vlan, the port must be in Hybrid mode. See portmode hybrid.
- VLAN stacking is not supported on Port Extender (PE) ports and on LAGs with port extender ports.
- VLAN stacking interface commands are blocked (hidden) on PE ports.
- VLAN stacking interface commands will fail on the VP-LAG (LAG with PE ports).

Topics:

- member
- vlan-stack access
- vlan-stack compatible
- vlan-stack dot1p-mapping
- vlan-stack protocol-type
- vlan-stack trunk

member

Assign a stackable VLAN access or trunk port to a VLAN. The VLAN must contain the `vlan-stack compatible` command in its configuration.

C9000 Series

Syntax

`member` *`interface`*

To remove an interface from a Stackable VLAN, use the `no member` *`interface`* command.

Parameters

interface Enter the following keywords and slot/port or number information:

- For a Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 10-Gigabit Ethernet interface, enter the keyword `TenGigabitEthernet` then the slot/port information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

Defaults

Not configured.

Command Modes

CONF-IF-VLAN

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.11.1	Introduced on the Z9000.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.

Usage Information

You must enable the stackable VLAN (using the `vlan-stack compatible` command) on the VLAN prior to adding a member to the VLAN.

Related Commands

vlan-stack compatible — enables stackable VLAN on a VLAN.

vlan-stack access

Specify a Layer 2 port or port channel as an access port to the stackable VLAN network.

C9000 Series

Syntax

`vlan-stack access`

To remove access port designation, use the `no vlan-stack access` command.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.

Usage Information

Prior to enabling this command, to place the interface in Layer 2 mode, enter the `switchport` command.

To remove the access port designation, remove the port (using the `no member interface` command) from all stackable VLAN enabled VLANs.

vlan-stack compatible

Enable the stackable VLAN feature on a VLAN.

C9000 Series

Syntax

`vlan-stack compatible`

To disable the Stackable VLAN feature on a VLAN, use the `no vlan-stack compatible` command.

Defaults

Not configured.

Command Modes CONF-IF-VLAN

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.

Usage Information Prior to disabling the stackable VLAN feature, remove the members.

To view the stackable VLANs, use the `show vlan` command in EXEC Privilege mode. Stackable VLANs contain members, designated by the M in the Q column of the command output.

Example

```
Dell#show vlan

Codes: * - Default VLAN, G - GVRP VLANs

   NUM  Status    Q Ports
*  1    Inactive
   2    Active    M Te 2/13
                  M Te 2/0-2
   3    Active    M Po1(Te 2/14-15)
                  M Te 2/18
                  M Te 2/3
   4    Active    M Po1(Te 2/14-15)
                  M Te 2/18
                  M Te 2/4
   5    Active    M Po1(Te 2/14-15)
                  M Te 2/18
                  M Te 2/5
Dell#
```

vlan-stack dot1p-mapping

Map C-Tag dot1p values to a S-Tag dot1p value. You can separate the C-Tag values by commas and dashed ranges are permitted. Dynamic mode CoS overrides any Layer 2 QoS configuration in case of conflicts.

C9000 Series

Syntax `vlan-stack dot1p-mapping c-tag-dot1p` *values* `sp-tag-dot1p` *value*

Parameters

c-tag-dot1p *value*	Enter the keyword `c-tag-dot1p` then the customer dot1p value that is mapped to a service provider do1p value. The range is from 0 to 7.
sp-tag-dot1p *value*	Enter the keyword `sp-tag-dot1p` then the service provider dot1p value. The range is from 0 to 7.

Defaults none

Command Modes INTERFACE

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Introduced on the C-Series and S-Series.

vlan-stack protocol-type

Define the stackable VLAN tag protocol identifier (TPID) for the outer VLAN tag (also called the VMAN tag). If you do not configure this command, the system assigns the value 0x9100.

C9000 Series

Syntax `vlan-stack protocol-type` *number*

Parameters

number	Enter the hexadecimal number as the stackable VLAN tag. You may specify both bytes of the 2-byte S-Tag TPID. The range is from 0 to FFFF. The default is **9100**.

Defaults 0x9100

Command Modes CONFIGURATION

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.

Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.
8.2.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.

Usage Information

For specific interoperability limitations regarding the S-Tag TPID, see the *Dell Networking OS Configuration Guide*.

The four characters you enter in the CLI for number are interpreted, as shown in the following table.

Number	Resulting TPID
1	0x0001
10	0x0010
81	0x0081
8100	0x8100

Related Commands

- portmode hybrid — sets a port (physical ports only) to accept both tagged and untagged frames. A port configured this way is identified as a hybrid port in report displays.
- vlan-stack trunk — specifies a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

vlan-stack trunk

Specify a Layer 2 port or port channel as a trunk port to the Stackable VLAN network.

C9000 Series

Syntax

```
vlan-stack trunk
```

To remove a trunk port designation from the selected interface, use the `no vlan-stack trunk` command.

Defaults

Not configured.

Command Modes

INTERFACE

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Netowrking OS version history for this command.

Version	Description
9.9(0.0)	Introduced on the C9010.
9.2(1.0)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.

Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.2.1.0	Introduced on the E-Series ExaScale. C-Series and S-Series accept both bytes of the 2-byte S-Tag TPID.
7.8.1.0	Functionality augmented for C-Series and S-Series to enable multi-purpose use of the port.
7.7.1.0	Functionality augmented for E-Series to enable multi-purpose use of the port.
7.6.1.0	Introduced on the C-Series and S-Series.

Usage Information

Prior to using this command, to place the interface in Layer 2 mode, execute the `switchport` command.

To remove the trunk port designation, first remove the port (using the `no member interface` command) from all stackable VLAN-enabled VLANs.

A VLAN-Stack trunk port is also allowed to be configured as a tagged port and as an untagged port for single-tagged VLANs. When the VLAN-Stack trunk port is also a member of an untagged VLAN, the port must be in Hybrid mode. Refer to portmode hybrid.

In Example 1, a VLAN-Stack trunk port is configured and then also made part of a single-tagged VLAN.

In Example 2, the tag protocol identifier (TPID) is set to 8848. The “Te 2/10” port is configured to act as a VLAN-Stack access port, while the “Te 1/0” port acts as a VLAN-Stack trunk port, switching stackable VLAN traffic for VLAN 10, while also switching untagged traffic for VLAN 30 and tagged traffic for VLAN 40. (To allow VLAN 30 traffic, the native VLAN feature is required, by executing the `portmode hybrid` command. Refer to portmode hybrid in Interfaces.

Example 1

```
Dell(conf-if-te-0/42)#switchport
Dell(conf-if-te-0/42)#vlan-stack trunk
Dell(conf-if-te-0/42)#show config
!
interface TenGigabitEthernet 0/42
  no ip address
  switchport
  vlan-stack trunk
  no shutdown
Dell(conf-if-te-0/42)#interface vlan 100
Dell(conf-if-vl-100)#vlan-stack compatible
Dell(conf-if-vl-100-stack)#member gigabitethernet 0/42
Dell(conf-if-vl-100-stack)#show config
!
interface Vlan 100
  no ip address
  vlan-stack compatible
  member TenGigabitEthernet 0/42
  shutdown
Dell(conf-if-vl-100-stack)#interface vlan 20
Dell(conf-if-vl-20)#tagged tengigabitethernet 0/42
Dell(conf-if-vl-20)#show config
!
interface Vlan 20
  no ip address
  tagged TenGigabitEthernet 0/42
  shutdown
Dell(conf-if-vl-20)#do show vlan
Codes: * - Default VLAN, G - GVRP VLANs
Q: U - Untagged, T - Tagged
```

```
   x - Dot1x untagged, X - Dot1x tagged
   G - GVRP tagged, M - Vlan-stack

  NUM  Status Description   Q Ports
* 1    Inactive
  20   Active               T Te 0/42
  100  Active               M Te 0/42
Dell(conf-if-vl-20)#
```

Example 2

```
Dell(config)#vlan-stack protocol-type 88A8
Dell(config)#interface tengigabitethernet 2/10
Dell(conf-if-te-2/10)#no shutdown
Dell(conf-if-te-2/10)#switchport
Dell(conf-if-te-2/10)#vlan-stack access
Dell(conf-if-te-2/10)#exit

Dell(config)#interface tenGigabitethernet 1/0
Dell(conf-if-te-1/0)#no shutdown
Dell(conf-if-te-1/0)#portmode hybrid
Dell(conf-if-te-1/0)#switchport
Dell(conf-if-te-1/0)#vlan-stack trunk
Dell(conf-if-te-1/0)#exit

Dell(config)#interface vlan 10
Dell(conf-if-vlan)#vlan-stack compatible
Dell(conf-if-vlan)#member Te 0/0, Te 1/0, Te 2/10
Dell(conf-if-vlan)#exit

Dell(config)#interface vlan 30
Dell(conf-if-vlan)#untagged TenGi 1/0
Dell(conf-if-vlan)#exit
Dell(config)#

Dell(config)#interface vlan 40
Dell(conf-if-vlan)#tagged TenGi 1/0
Dell(conf-if-vlan)#exit
Dell(config)#
```

68

X.509v3

X.509v3 is a standard for public key infrastructure (PKI) to manage digital certificates and public key encryption. This standard specifies a format for public-key certificates or digital certificates.

Dell Networking OS supports X.509v3 standards.

Topics:

- crypto ca-cert delete
- crypto ca-cert install
- crypto cert delete
- crypto cert generate
- crypto cert install
- crypto x509 ocsp
- crypto x509 revocation
- debug crypto
- logging secure
- crypto x509 ca-keyid
- ocsp-server
- ocsp-server prefer
- show crypto ca-cert
- show crypto cert

crypto ca-cert delete

Deletes a CA certificate.

Syntax `crypto ca-cert delete [index]`

Parameters

index	(Optional) Enter the keyword `index` to specify the index of the CA certificate. If index is not specified, the system deletes all of the installed CA certificates.

Defaults NA.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced the command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

Before deleting a CA certificate, the system checks whether that certificate is an issuer of other installed certificate on the system. If so, the system informs you to delete other installed certificates first.

Related Commands

crypto ca-cert installcrypto cert generatecrypto ca-cert install

crypto ca-cert install

Downloads and installs the certificate of a Certificate Authority (CA) on to the device.

Syntax

```
crypto ca-cert install path
```

Parameters

path

Enter the path where the CA certificate is available for download. The format that you use to specify the location of the CA certificate also includes the protocol that is used to contact the CA. You can use the following options that you can use to download and install a certificate from the CA:

- tftp — `tftp://ca-ip-address/tftp/CAcert.pem`
- usbflash: — `usbflash:/certs/CAcert.pem`
- ftp — `ftp://userid:password@ca-ip-address/certs/CAcert.pem`
- scp — `scp://userid:password@ca-ip-address/certs/CAcert.pem`
- http — `http://192.168.1.100/certs/CAcert.pem`
- flash — `flash://filepath/filename`

Defaults

NA.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced the command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

Upon successful installation, the system displays a notification on the device. If remote logging is configured, the notification is also sent to the syslog server. Contents of the CA certificate's subject are displayed.

Related Commands

- crypto cert install

crypto cert delete

Deletes a trusted certificate.

Syntax

```
crypto cert delete
```

Defaults

NA.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced the command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

The certificate matching the current FIPS state is deleted. If the system is in FIPS mode, the FIPS certificate is deleted. If the system is in non-FIPS mode, the non-FIPS certificate is deleted.

Before deleting the system's trusted certificate, the system prompts you to specify whether to proceed with deletion. If you proceed, the system deletes the certificate and also the private key.

Related Commands

- crypto ca-cert install
- crypto cert generate

crypto cert generate

Generates a Certificate Signing Request (CSR) or a self-signed certificate.

Syntax

```
crypto cert generate {self-signed | request} [cert-file cert-path key-file
{private | key-path}] [country 2-letter code] [state state] [locality city]
[organization organization-name] [orgunit unit-name] [cname common-name] [email
email-address] [validity days] [length length] [altname alt-name]
```

Parameters

self-signed Enter the keyword `self-signed` to create a self-signed certificate.

request Enter the keyword `request` to create a certificate signing request.

cert-file Enter the keyword `cert-file` to specify that the certificate needs to be created.

NOTE: If the cert-file option is not specified in the command, then the system interactively prompts you to fill in rest of the fields of the certificate signing request (CSR).

cert-path	Enter the path to locally store the self-signed certificate or CSR. The path can be a full path or a relative path. If the system accepts this path, a notification is sent indicating the location where the CSR file is stored. You can then export the CSR to a CA using the "copy" command. Following is an example of a path that you can specify: `flash://certs/s4810-001-request.csr`.
key-file	Enter the keyword `key-file` to specify the private key.
private	Enter the keyword private to specify that the key is stored in a hidden location in the NVRAM. Only one private key can exist in a hidden location at any given point in time.
key-path	Enter the absolute or relative location on the device where the key is stored.
country *2–letter-code*	(OPTIONAL) Enter the keyword `country` followed by the two letter code that is used to identify the country name.
state *state*	(OPTIONAL) Enter the keyword `state` followed by the name of the state.
locality *city*	(OPTIONAL) Enter the keyword *locality* followed by the name of the city.
organization *organization-name*	(OPTIONAL) Enter the keyword `organization` followed by the name of the organization.
orgunit *unit-name*	(OPTIONAL) Enter the keyword `orgunit` followed by the name of the unit.
cname *common-name*	Enter the keyword `cname` followed by the common name that you want to assign. **NOTE: Common Name is an important attribute while creating a CSR or a self-signed certificate. Common name is the main identity presented to connecting entities. By default, the device's host name acts as the common name. However, you can still configure a different common name for the device. For example, you can specify an IP address to act as a Common Name for the device. If the Common Name does not match the device's presented identity, then even a properly signed certificate does not validate correctly.**
email *email-address*	(OPTIONAL) Enter the keyword `email` followed a valid email address used for communication with the organization.
validity *days*	(OPTIONAL) Enter the keyword `validity` followed by the number of days for which the certificate is valid. **NOTE: For CSRs, validity has no effect. For self-signed certificates, if validity is not specified, it defaults to 3650 days, or 10 years.**
length *length*	(OPTIONAL) Enter the keyword `length` followed by a bit length value. The default key length for both FIPS and non-FIPS mode is 2048. Minimum key length value for FIPS mode is 2048. The range is from 2048 to 4096. Minimum key length value for non-FIPS mode is 1024. The range is from 1024 to 4096.
altname *altname*	(OPTIONAL) Enter the keyword `altname` followed by the subject alternate name for the organization. For example, `altname IP:192.168.1.100`.

Defaults NA.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced the command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

If the cert-file option is not specified in the command, then the system interactively prompts you to fill in various fields of the certificate signing request (CSR). You are prompted to fill out some metadata information for the certificate. The following example shows the fields that you are prompted to fill:

```
You are about to be asked to enter information that will be incorporated into
your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank.
For some fields there will be a default value; if you enter '.', the field
will be left blank.
-----
Country Name (2 letter code) [US]:
State or Province Name (full name) [Some-State]:California
Locality Name (eg, city) []:San Francisco
Organization Name (eg, company) []:Starfleet Command
Organizational Unit Name (eg, section) []:NCC-1701A
Common Name (eg, YOUR name) [S4810-001]:
Email Address []:scotty@starfleet.com
```

You can enter only 256 characters per command. If you have field values that are larger than 256 characters in length, use the interactive mode of the command.

Related Commands

- crypto ca-cert install

crypto cert install

Installs a trusted certificate on a device.

Syntax

```
crypto cert install cert-file cert-path key-file {key-path | private} [password passphrase]
```

Parameters

cert-file	Enter the keyword `cert-file` to specify that the certificate needs to be downloaded.
cert-path	Enter the path where the certificate is locally stored. The path can be a full path or a relative path. If the system accepts this path, a notification is sent indicating the location where the certificate file is stored. Following are example of a path that you can specify: `flash://certs/s4810-001-request.crt`and `usbflash:/certs/s4810-001-cert.pem` **NOTE: Before installing a trusted certificate, you first need to download it from a remote CA using the copy command.** .
key-file	Enter the keyword `key-file` to specify the private key.
private	Enter the keyword private to specify that the key is stored in a hidden location in the NVRAM. Only one private key can exist in a hidden location at any given point in time.
key-path	Enter the absolute or relative location on the device where the key is stored.

NOTE: After the certificate is successfully installed, the private key is deleted from the specified location and copied to the hidden location in NVRAM.

password *passphrase*	(Optional) Enter the keyword `password` followed by the password phrase used to decrypt the private key.

NOTE: You can generate the private key and certificate on another host. While doing so, you must keep the private key encrypted with a passphrase so that the private key is not compromised during transport. The password phrase acts a facility to decrypt the private key before installing it on the switch.

Defaults

NA.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command.

Version	Description
9.11.0.0	Introduced the command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

Certain parameters must be met in order for this command to succeed:

- The downloaded certificate should be formatted properly.
- In order for verification to work, the CA certificate must be installed on the system before running this command.
- The downloaded certificate's public key must correspond to the private key.
- If the certificate is not self-signed, then the CA certificate (from the CA that has signed the certificate) must be installed on the system prior to running this command for verification to work.

NOTE: It is possible for the switch to store two types of certificates: one for the FIPS mode and one for the non-FIPS mode. If the system is in FIPS mode, the certificate is installed as the FIPS certificate. If the system is in non-FIPS mode, the certificate is installed as the non-FIPS certificate. When FIPS mode is enabled or disabled, the certificates (and keys) are switched by the system.

NOTE: For the switch, there are two possible certificates stored - one for FIPS mode, one for non-FIPS mode. If the system is in FIPS mode, the certificate will be installed as the FIPS certificate. If the system is in non-FIPS mode, the certificate will be installed as the non-FIPS certificate. When FIPS mode is enabled/disabled, the certificates (and keys) are switched by the system.

Related Commands

- crypto ca-cert install

crypto x509 ocsp

Configures the OCSP behavior.

Syntax

```
crypto x509 ocsp [nonce] [sign-requests]
```

Parameters

nonce	Enter the keyword `nonce` to use the nonce feature for the OCSP requests to OCSP responder communication. This is a one-time value that must be returned in the OCSP response. If the OCSP responder is using precomputed responses, then it does not reply with the nonce. The nonce feature is off by default. The no version of the command disables the nonce feature.
sign-requests	Enter the keyword `sign-requests` to sign the OCSP requests to OCSP responder communication with the system's own certificate so that the OCSP responder may verify the requestor. The sign-requests feature is off by default. The no version of the command disables signing of requests.

Defaults

NA.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced the command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

Related Commands

- crypto ca-cert install
- crypto cert generate
- crypto cert install

crypto x509 revocation

Configure the revocation check behavior for the certificate.

Syntax

```
crypto x509 revocation ocsp {accept | reject}
```

Parameters

ocsp	Enter the method used to check certificate revocation details. In this release, OCSP is the only option that is supported. So, you can specify OCSP as the method-list value.
accept	Enter the keyword `accept` to accept the presented certificate and log in if OCSP retrieval fails.

	reject	Enter the keyword `reject` to reject the presented certificate and log in if OCSP retrieval fails.

Defaults crypto x509 revocation ocsp accept

Command Modes

- CONFIGURATION Mode

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced this command.

Related Commands

- crypto x509 ocsp

debug crypto

This command allows you to test a certificate chain file for validity and checking revocation outside of its use in TLS communication.

Syntax `debug crypto {flash://path}`

Parameters

path	Enter the path to a local file where a certificate chain is stored in PEM format.

Defaults None.

Command Modes EXEC Privilege

Command History This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced this command.

Usage Information The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

You can use this command to verify an X509 certificate outside of use with Syslog over TLS.

Related Commands

- crypto cert install
- crypto cert generate
- crypto ca-cert install

logging secure

Creates a log file for various events related to X.509v3 certificates.

Syntax

```
logging {hostname} {secure | tcp | udp} [vrf vrf-name] [sha1 fingerprint] [port port-number]
```

Parameters

hostname	Enter the name of the host or device for which you wish to record logs corresponding to the certificates. **NOTE: The hostname can be an IPV4 address, an IPV6 address, or a DNS hostname—with or without DNS suffix.**
secure	Enter the keyword `secure` to enable the Syslog feature to communicate with a compatible Syslog server using the secure TLS protocol over the default port (6514). The range is from 1024 to 65535.
tcp	Enter the keyword `tcp` to enable TCP.
udp	Enter the keyword `udp` to enable UDP.
vrf *vrf-name*	Enter the keyword `vrf` followed by the name of the VRF.
sha1 *fingerprint*	Enter the keyword `sha1` followed by the finger print. This option is only available when the secure option is configured. This new option enables the Syslog feature to compare the received certificate's sha-1 fingerprint against this configured sha-1 fingerprint. If present, only the fingerprint is used for certificate revocation validation.
port *port-number*	Enter the keyword `port` followed by the port number. The default port number is 6514 for secure logging.

Defaults

None.

Command Modes

CONFIGURATION

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced this command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

Following are the pre-requisites to configure logging:

- The logging command must be configured to enable event logging.
- A certificate must be installed on the switch. This certificate is only used for secure logging.
- At least one CA certificate must be installed on the switch so that the logging server's certificate can be verified. If a SHA1 fingerprint is present, only the fingerprint is used for certificate revocation validation.

Related Commands

- crypto cert install
- crypto ca-cert install
- crypto cert generate

crypto x509 ca-keyid

Creates a per-certificate configuration context using the specified subject key identifier.

Syntax

`crypto x509 ca-keyid` *`subject-key-identifier`*

Use to the `no crypto x509 ca-keyid` command to remove this configuration.

Parameters

subject-key-identifier	Enter the content of the `SubjectKeyIdentifier` field from the CA certificate. **NOTE: To get the subject key identifier details, enter the `show crypto ca-cert` command. This command displays the CA certificate details.**

Defaults

None.

Command Modes

- CONFIGURATION Mode

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced this command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

When you use this command, the device maps the current certificate context in the certificate store to a CA certificate through the subject key identifier field. The subject key identifier field contains the SHA-1 hash of the CA's public key. This configuration provides a way to uniquely identify a CA and associate it with any CA-specific settings.

This context is used to store certificate-specific settings such as alternate CRL and OCSP locations. Incoming X.509 certificates whose `AuthorityKeyIdentifier`extensions match the configured subject key identifier has these settings applied to them.

The `crypto x509 ca-keyid` command when used with the `ocsp-server` command in the global configuration mode creates a per-certificate configuration context under which the remaining commands are entered.

Related Commands

- ocsp-server
- crypto x509 ocsp

ocsp-server

Configures OCSP server on a CA.

Syntax

```
ocsp-server url [nonce] [sign-requests]
```

Parameters

url	Enter the URL for the OCSP responder using standard URI format. Either http or https protocol can be used. For example, http://[1100::101]:8888.
nonce	Enter the keyword `nonce` to use the nonce feature for the OCSP requests to OCSP responder communication. This number is a one-time value that must be returned in the OCSP response. If the OCSP responder is using precomputed responses, then it does not reply with the nonce. The nonce feature is off by default. The no version of the command disables the nonce feature.
sign-requests	Enter the keyword `sign-requests` to sign the OCSP requests to OCSP responder communication with the system's own certificate so that the OCSP responder may verify the requestor. The sign-requests feature is off by default. The no version of the command disables signing of requests.

Defaults

None.

Command Modes

CERTIFICATE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced this command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

Multiple OCSP responders may be configured per CA. The system tries each one until it gets a valid response. No priority may be specified or guaranteed; the system tries them in the order in which they were configured.

Related Commands

- crypto x509 ocsp

ocsp-server prefer

Configures OCSP responder preference. You can configure the preference or order that the CA or a device should follow while contacting multiple OCSP responders.

Syntax

```
ocsp-server prefer
```

Defaults

None.

Command Modes

CERTIFICATE

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced this command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

When this command is specified, the system checks the configured OCSP URLs before checking the URL of the OCSP server in the authorityInfoAccess extension of the certificate. If this command is not specified, then the system checks the OCSP server in the authorityInfoAccess extension of the certificate before checking the configured OCSP servers.

Related Commands

- crypto x509 ocsp

show crypto ca-cert

Displays the certificate information corresponding to the root CA.

Syntax

```
show crypto ca-certs
```

Defaults

None.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced this command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

This show command should display the index, the certificate's subject field in plaintext, not-before and not-after dates, and the fingerprint in hexadecimal format. The index assigned to each CA certificate is used by the crypto cert delete certificate-authority command to allow the user to specify which certificate authority to remove.

Related Commands

- crypto ca-cert install

show crypto cert

Displays the certificate information that is specified.

Syntax

```
show crypto cert {path}
```

Parameters

path	(OPTIONAL) Enter the path to a local file where a certificate chain is stored in PEM format. If a path is not specified, display the certificate that is currently installed on the system.

Defaults

None.

Command Modes

EXEC Privilege

Command History

This guide is platform-specific. For command information about other platforms, see the relevant *Dell Networking OS Command Line Reference Guide*.

The following is a list of the Dell Networking OS version history for this command:

Version	Description
9.11.0.0	Introduced this command.

Usage Information

The following RBAC roles are allowed to issue this command:

- sysadmin
- secadmin

Related Commands

- crypto cert install