

Dell Command Line Reference Guide for the S6000– ON System

9.8(0.0)



Notes, cautions, and warnings



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



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.

Contents

1 About this Guide.....	37
Objectives.....	37
Audience.....	37
Conventions.....	37
Information Icons.....	38
2 CLI Basics.....	39
Accessing the Command Line.....	39
Multiple Configuration Users.....	39
Obtaining Help.....	40
Navigating the CLI.....	41
Using the Keyword no Command.....	42
Filtering show Commands.....	42
Enabling Software Features on Devices Using a Command Option.....	43
feature vrf.....	43
show feature.....	44
Command Modes.....	44
3 File Management.....	52
boot system.....	52
cd.....	53
HTTP Copy via CLI.....	54
copy.....	55
delete.....	57
dir.....	58
format (S-Series).....	60
fsck flash.....	60
mkdir.....	61
mount nfs.....	62
rmdir.....	62
upgrade system.....	63
rename.....	64
show boot system.....	64
show bootvar.....	65
show file-systems.....	66
show os-version.....	67
show running-config.....	68
show startup-config.....	72
show version.....	72
upgrade system.....	74
upgrade boot.....	75
verify.....	77



4 Control and Monitoring.....	78
banner exec.....	78
banner login.....	79
banner motd.....	81
cam-acl.....	82
clear line.....	83
configure.....	84
disable.....	84
do.....	85
enable.....	86
enable optic-info-update interval.....	87
end.....	88
exec-timeout.....	89
exit.....	89
ftp-server enable.....	90
ftp-server topdir.....	91
ftp-server username.....	92
hostname.....	93
ip ftp password.....	94
ip ftp source-interface.....	95
ip tftp vrf.....	96
ip ftp username.....	96
ip ftp vrf.....	97
ip telnet server enable.....	98
ip telnet server vrf.....	98
ip telnet source-interface.....	99
ip tftp vrf.....	100
line.....	101
login concurrent-session.....	102
login statistics.....	103
motd-banner.....	105
ping.....	105
reload.....	108
send.....	109
service timestamps.....	110
show alarms.....	111
show command-tree.....	112
show cpu-traffic-stats.....	113
show debugging.....	114
show environment.....	115
show inventory.....	116
show login statistics.....	118
show memory.....	120
show processes cpu.....	121
show processes ipc flow-control.....	124

show processes memory.....	126
show software ifm.....	128
show system.....	129
show tech-support.....	133
ssh-peer-stack-unit.....	136
telnet.....	136
telnet-peer-stack-unit.....	138
terminal length.....	139
traceroute.....	139
undebg all.....	141
virtual-ip.....	142
write.....	143

5 802.1X.....144

debug dot1x.....	144
dot1x auth-fail-vlan.....	145
dot1x auth-server.....	146
dot1x auth-type mab-only.....	147
dot1x authentication (Configuration).....	147
dot1x authentication (Interface).....	148
dot1x guest-vlan.....	149
dot1x host-mode.....	150
dot1x mac-auth-bypass.....	150
dot1x max-eap-req.....	151
dot1x max-suplicants.....	152
dot1x port-control.....	152
dot1x quiet-period.....	153
dot1x reauthentication.....	154
dot1x reauth-max.....	154
dot1x server-timeout.....	155
dot1x supplicant-timeout.....	156
dot1x tx-period.....	157
show dot1x cos-mapping interface.....	157
show dot1x interface.....	159

6 Access Control Lists (ACL).....163

Commands Common to all ACL Types.....	163
remark.....	163
show config.....	164
Common IP ACL Commands.....	165
access-class.....	165
clear counters ip access-group.....	166
ip access-group.....	167
ip control-plane egress-filter.....	168
show ip accounting access-list.....	169
Standard IP ACL Commands.....	170



deny.....	170
ip access-list standard.....	172
permit.....	173
resequence access-list.....	174
seq.....	175
Extended IP ACL Commands.....	176
deny.....	177
deny icmp.....	178
deny tcp.....	180
deny udp.....	182
ip access-list extended.....	185
permit.....	186
permit tcp.....	187
permit udp.....	190
resequence access-list.....	192
seq.....	193
Common MAC Access List Commands.....	195
clear counters mac access-group.....	195
mac access-group.....	196
show mac access-lists.....	197
show mac accounting access-list.....	198
Standard MAC ACL Commands.....	199
deny.....	199
mac access-list standard.....	201
permit.....	202
seq.....	203
Extended MAC ACL Commands.....	204
deny.....	205
mac access-list extended.....	206
permit.....	208
IP Prefix List Commands.....	209
clear ip prefix-list.....	209
deny.....	210
ip prefix-list.....	211
seq.....	212
show config.....	213
show ip prefix-list detail.....	213
show ip prefix-list summary.....	214
Route Map Commands.....	215
continue.....	215
description.....	216
match as-path.....	217
match community.....	218
match interface.....	218
match ip address.....	220

match ip next-hop.....	220
match ip route-source.....	221
match metric.....	222
match origin.....	223
match route-type.....	224
match tag.....	225
route-map.....	226
set as-path.....	227
set automatic-tag.....	228
set comm-list delete.....	228
set community.....	229
set level.....	230
set local-preference.....	231
set metric.....	232
set metric-type.....	233
set next-hop.....	234
set origin.....	235
set tag.....	235
set weight.....	236
show config.....	237
show route-map.....	238
deny (for Standard IP ACLs).....	239
deny (for Extended IP ACLs).....	240
seq (for Standard IPv4 ACLs).....	241
deny tcp (for Extended IP ACLs).....	242
deny ether-type (for Extended MAC ACLs).....	244
deny (for Standard MAC ACLs).....	245
deny (for Extended MAC ACLs).....	246
permit (for Standard IP ACLs).....	248
permit arp (for Extended MAC ACLs).....	249
permit ether-type (for Extended MAC ACLs).....	250
permit icmp (for Extended IP ACLs).....	251
permit udp (for Extended IP ACLs).....	253
permit (for Extended IP ACLs).....	254
permit (for Standard MAC ACLs).....	255
seq (for Standard MAC ACLs).....	257
permit tcp (for Extended IP ACLs).....	258
seq arp (for Extended MAC ACLs).....	259
seq ether-type (for Extended MAC ACLs).....	260
seq (for IP ACLs).....	262
seq (for IPv6 ACLs).....	263
permit udp (for IPv6 ACLs).....	264
permit tcp (for IPv6 ACLs).....	265
permit icmp (for IPv6 ACLs).....	267
permit (for IPv6 ACLs).....	268



deny udp (for IPv6 ACLs).....	269
deny arp (for Extended MAC ACLs).....	271
deny tcp (for IPv6 ACLs).....	272
deny icmp (for Extended IPv6 ACLs).....	273
deny (for IPv6 ACLs).....	274
7 Bidirectional Forwarding Detection (BFD).....	276
bfd all-neighbors.....	276
ip route bfd.....	277
neighbor bfd.....	278
neighbor bfd disable.....	279
8 Boot Command Line Interface.....	281
boot change.....	281
boot message.....	282
boot show net config retries.....	283
boot write net config retries.....	283
boot zero.....	283
default-gateway.....	284
etheraddr <macaddr>.....	285
ignore enable-password.....	285
ignore startup-config.....	286
interface management ethernet ip address.....	286
NVRAM erase.....	287
reload.....	287
serial console.....	287
show bootvar.....	288
show default-gateway.....	289
show interface management ethernet.....	289
show serial console baud rate.....	290
watchdog <string>.....	290
9 Border Gateway Protocol.....	292
BGP IPv4 Commands.....	292
address-family.....	292
aggregate-address.....	293
bgp add-path.....	295
bgp always-compare-med.....	295
bgp asnotation.....	296
bgp bestpath as-path ignore.....	297
bgp bestpath as-path multipath-relax.....	298
bgp bestpath med confed.....	298
bgp bestpath med missing-as-best.....	299
bgp bestpath router-id ignore.....	300
bgp client-to-client reflection.....	300
bgp cluster-id.....	301

bgp confederation identifier.....	302
bgp confederation peers.....	303
bgp dampening.....	304
bgp default local-preference.....	305
bgp dmzlink-bw.....	306
bgp enforce-first-as.....	307
bgp fast-external-fallover.....	307
bgp four-octet-as-support.....	308
bgp graceful-restart.....	309
bgp non-deterministic-med.....	310
bgp recursive-bgp-next-hop.....	311
bgp regex-eval-optz-disable.....	311
bgp router-id.....	313
clear ip bgp.....	313
clear ip bgp dampening.....	315
clear ip bgp flap-statistics.....	316
clear ip bgp peer-group.....	317
debug ip bgp.....	318
debug ip bgp dampening.....	319
debug ip bgp events.....	320
debug ip bgp keepalives.....	321
debug ip bgp notifications.....	322
debug ip bgp soft-reconfiguration.....	323
debug ip bgp updates.....	324
default-metric.....	325
deny bandwidth.....	326
description.....	326
maximum-paths.....	327
neighbor activate.....	327
neighbor add-path.....	328
neighbor advertisement-interval.....	329
neighbor advertisement-start.....	330
neighbor allowas-in.....	331
neighbor default-originate.....	331
neighbor description.....	333
neighbor distribute-list.....	333
neighbor ebgp-multihop.....	334
neighbor fall-over.....	335
neighbor local-as.....	336
neighbor maximum-prefix.....	337
neighbor password.....	338
neighbor peer-group (assigning peers).....	339
neighbor peer-group (creating group).....	340
neighbor peer-group passive.....	341
neighbor remote-as.....	342

neighbor remove-private-as.....	343
neighbor route-map.....	344
neighbor route-reflector-client.....	345
neighbor send-community.....	346
neighbor shutdown.....	347
neighbor soft-reconfiguration inbound.....	348
neighbor timers.....	349
neighbor update-source.....	350
neighbor weight.....	351
network.....	351
network backdoor.....	353
permit bandwidth.....	354
redistribute.....	354
redistribute ospf.....	355
router bgp.....	356
set extcommunity bandwidth.....	357
show capture bgp-pdu neighbor.....	358
show config.....	359
show ip bgp.....	359
show ip bgp cluster-list.....	361
show ip bgp community.....	363
show ip bgp community-list.....	365
show ip bgp dampened-paths.....	367
show ip bgp detail.....	368
show ip bgp extcommunity-list.....	370
show ip bgp filter-list.....	371
show ip bgp flap-statistics.....	373
show ip bgp inconsistent-as.....	375
show ip bgp neighbors.....	376
show ip bgp next-hop.....	380
show ip bgp paths.....	381
show ip bgp paths community.....	382
show ip bgp peer-group.....	383
show ip bgp regexp.....	385
show ip bgp summary.....	386
show running-config bgp.....	389
timers bgp.....	390
MBGP Commands.....	390
debug ip bgp dampening.....	391
distance bgp.....	392
show ip bgp dampened-paths.....	393

10 Content Addressable Memory (CAM).....395

CAM Profile Commands.....	395
cam-acl (Configuration).....	395
cam-acl-egress.....	398

cam-optimization.....	399
show cam-acl.....	399
test cam-usage.....	401
Unified Forwarding Table Modes.....	403
hardware forwarding-table mode.....	403
show hardware forwarding-table mode.....	403

11 Control Plane Policing (CoPP)..... 405

control-plane-cpuqos.....	405
service-policy rate-limit-cpu-queues.....	405
service-policy rate-limit-protocols.....	406
show cpu-queue rate cp.....	407
show ip protocol-queue-mapping.....	408
show ipv6 protocol-queue-mapping.....	409
show mac protocol-queue-mapping.....	409

12 Data Center Bridging (DCB).....411

DCB Command.....	411
dcb-enable.....	411
PFC Commands.....	412
clear pfc counters.....	412
pfc no-drop queues.....	413
pfc priority.....	414
show dcb.....	414
show interface pfc.....	415
show interface pfc statistics.....	417
ETS Commands.....	418
dcb-enable.....	418
clear ets counters.....	419
show interface ets.....	420
DCBX Commands.....	423
advertise dcbx-tlv.....	424
dcbx port-role.....	424
dcbx version.....	425
debug dcbx.....	426
fcoe priority-bits.....	427
iscsi priority-bits.....	427
show interface dcbx detail.....	428
dcb-map.....	430
priority-pgid.....	431
priority-group bandwidth pfc.....	432
dcb-map stack-unit all stack-ports all.....	433
dcb pfc-shared-buffer-size.....	434
dcb-buffer-threshold	435
priority.....	435
qos-policy-buffer.....	436



dcb-policy buffer-threshold (Interface Configuration).....	438
show qos dcb-buffer-threshold.....	438
dcb pfc-total-buffer-size.....	439
show running-config dcb-buffer-threshold.....	440
dcb pfc-queues.....	441
dcb {ets pfc} enable.....	442

13 Debugging and Diagnostics.....443

Diagnostics and Monitoring Commands.....	443
logging coredump stack-unit.....	443
Offline Diagnostic Commands.....	444
diag stack-unit.....	444
offline stack-unit.....	445
online stack-unit.....	446
Hardware Commands.....	447
clear hardware stack-unit.....	447
clear hardware system-flow.....	448
clear hardware vlan-counters.....	448
hardware watchdog.....	449
show hardware layer2.....	449
show hardware layer3.....	450
show hardware stack-unit.....	451
show hardware stack-unit buffer.....	459
show hardware buffer-stats-snapshot.....	461
show hardware counters interface	463
show hardware drops.....	465
show hardware system-flow.....	466
show hardware vlan-counters.....	468
show hardware stack-unit buffer-stats-snapshot	469
show hardware stack-unit buffer-stats-snapshot (Total Buffer Information).....	471

14 Dynamic Host Configuration Protocol (DHCP).....473

Commands to Configure the System to be a DHCP Server.....	473
clear ip dhcp.....	473
debug ip dhcp server.....	474
debug ipv6 dhcp	474
default-router.....	475
disable.....	475
dns-server.....	476
domain-name.....	476
excluded-address.....	477
hardware-address.....	478
host.....	478
lease.....	479
netbios-name-server.....	479
netbios-node-type.....	480

network.....	481
pool.....	481
show ip dhcp binding.....	482
show ip dhcp configuration.....	482
show ip dhcp conflict.....	483
show ip dhcp server.....	483
Commands to Configure Secure DHCP.....	484
arp inspection.....	484
arp inspection-trust.....	484
clear ip dhcp snooping.....	485
clear ipv6 dhcp snooping binding.....	486
ip dhcp relay.....	487
ip dhcp snooping.....	487
ipv6 dhcp snooping.....	488
ipv6 dhcp snooping vlan.....	488
ip dhcp snooping binding.....	489
IPv6 DHCP Snooping Binding.....	490
ip dhcp snooping database.....	491
ipv6 dhcp snooping database write-delay.....	491
ip dhcp snooping database renew.....	492
ipv6 dhcp snooping database renew.....	492
ip dhcp snooping trust.....	493
ipv6 dhcp snooping trust.....	493
ip dhcp source-address-validation.....	493
ip dhcp relay information-option.....	494
ip dhcp snooping verify mac-address.....	495
ipv6 dhcp snooping verify mac-address.....	496
ip helper-address.....	496
ipv6 helper-address.....	497
show ip dhcp snooping.....	497
show ipv6 dhcp snooping.....	499
Commands to Configure DNS	500
ip name-server.....	500
ip domain-name.....	501
ip domain-list.....	502
ip host.....	502
clear host.....	503

15 Equal Cost Multi-Path (ECMP)..... 504

ecmp-group.....	504
hash-algorithm.....	505
ip ecmp-group.....	508
ip ecmp weighted.....	508
link-bundle-distribution trigger-threshold.....	509
link-bundle-monitor enable.....	510



16 Flex Hash and Optimized Boot-Up.....	511
load-balance ingress-port enable.....	511
load-balance flexhash.....	511
reload-type fastboot.....	513
lacp fast-switchover.....	513
encapsulation dot1q.....	514
17 FIP Snooping.....	515
clear fip-snooping database interface vlan.....	515
clear fip-snooping statistics.....	516
debug fip snooping.....	516
debug fip snooping rx.....	517
feature fip-snooping.....	518
fip-snooping enable.....	518
fip-snooping fc-map.....	519
fip-snooping max-sessions-per-enodemac.....	520
fip-snooping port-mode fcf.....	520
fip-snooping port-mode fcoe-trusted.....	521
show fip-snooping config.....	521
show fip-snooping enode.....	522
show fip-snooping fcf.....	523
show fip-snooping statistics.....	524
show fip-snooping system.....	526
show fip-snooping vlan.....	527
show fips status.....	528
18 Force10 Resilient Ring Protocol (FRRP).....	529
clear frrp.....	529
debug frrp.....	530
description.....	531
disable.....	532
interface.....	532
member-vlan.....	534
mode.....	534
protocol frrp.....	535
show frrp.....	536
timer.....	537
19 GARP VLAN Registration (GVRP).....	539
clear gvrp statistics.....	540
debug gvrp.....	540
disable.....	541
garp timers.....	542
gvrp enable.....	543
gvrp registration.....	544

protocol gvrp.....	545
show config.....	546
show garp timers.....	546
show gvrp.....	547
show gvrp statistics.....	548

20 ICMP Message Types.....550

21 Internet Group Management Protocol (IGMP).....552

IGMP Commands.....	552
clear ip igmp groups.....	552
debug ip igmp.....	553
ip igmp access-group.....	554
ip igmp immediate-leave.....	555
ip igmp last-member-query-interval.....	556
ip igmp query-interval.....	556
ip igmp query-max-resp-time.....	557
ip igmp ssm-map.....	558
ip igmp version.....	559
show ip igmp groups.....	560
show ip igmp interface.....	562
show ip igmp ssm-map.....	563
IGMP Snooping Commands.....	564
clear ip igmp snooping groups.....	565
debug ip igmp snooping.....	565
ip igmp snooping enable.....	566
ip igmp snooping fast-leave.....	567
ip igmp snooping last-member-query-interval.....	568
ip igmp snooping mrouter.....	569
ip igmp snooping querier.....	570
show ip igmp snooping groups.....	570
show ip igmp snooping mrouter.....	572

22 Interfaces.....573

Basic Interface Commands.....	573
clear counters.....	573
clear dampening.....	574
dampening.....	575
description.....	577
duplex (10/100 Interfaces).....	578
flowcontrol.....	578
interface.....	581
interface group.....	582
interface loopback.....	583
interface ManagementEthernet.....	584
interface null.....	585



interface range.....	586
interface range macro (define).....	588
interface range macro name.....	590
interface vlan.....	591
intf-type cr4 autoneg.....	592
keepalive.....	593
monitor interface.....	593
mtu.....	596
negotiation auto.....	598
portmode hybrid.....	600
rate-interval.....	601
show config.....	602
show config (for speed).....	603
show config (from INTERFACE RANGE mode).....	603
show interfaces.....	604
show interfaces configured.....	610
show interfaces dampening.....	611
show interfaces stack-unit.....	612
show interfaces status.....	613
show interfaces vlan.....	614
show system stack-unit quad-port-profile.....	615
stack-unit quad-port-profile.....	616
show interfaces switchport.....	616
show interfaces transceiver.....	618
show range.....	623
shutdown.....	623
speed (Management interface).....	624
stack-unit portmode.....	625
switchport.....	626
Port Channel Commands.....	628
channel-member.....	628
group.....	629
interface port-channel.....	630
minimum-links.....	632
port-channel failover-group.....	632
show interfaces port-channel.....	633
show port-channel-flow.....	636
Enhanced Validation of Interface Ranges.....	637
ip http source-interface.....	637

23 IPv4 Routing..... 639

arp.....	639
arp backoff-time.....	640
arp learn-enable.....	641
arp max-entries.....	642
arp retries.....	642

arp timeout.....	643
clear arp-cache.....	644
clear host.....	645
clear ip fib stack-unit.....	645
clear ip route.....	646
clear tcp statistics.....	647
debug arp.....	648
debug ip dhcp.....	649
debug ip icmp.....	650
debug ip packet.....	652
ip address.....	654
ip directed-broadcast.....	655
ip domain-list.....	656
ip domain-lookup.....	657
ip domain-name.....	658
ip helper-address.....	659
ip helper-address hop-count disable.....	660
ip host.....	660
ip icmp source-interface.....	661
ipv6 icmp source-interface.....	662
ip max-frag-count.....	664
ip name-server.....	664
ip proxy-arp.....	665
ip route.....	666
ip source-route.....	668
ip tcp initial-time.....	669
ip unknown-unicast.....	670
ipv4 unicast-host-route.....	670
show ip tcp initial-time.....	671
ip unreachable.....	671
load-balance.....	672
load-balance hg.....	673
management route.....	675
show arp.....	676
show arp retries.....	679
show hosts.....	679
show ip cam stack-unit.....	681
show ip fib stack-unit.....	683
show ip flow.....	684
show ip interface.....	686
show ip management-route.....	688
show ipv6 management-route.....	689
show ip protocols.....	690
show ip route.....	691
show ip route list.....	695



show ip route summary.....	696
show ip traffic.....	697
show tcp statistics.....	699

24 IPv6 Basics..... 702

cam-ipv6 extended-prefix.....	702
clear ipv6 route.....	702
maximum dynamic-routes-ipv6.....	703
show cam-ipv6 extended-prefix.....	704
ipv6 unicast-host-route.....	705
ipv6 nd dns-server	705
ipv6 route.....	706
show ipv6 route.....	708

25 IPv6 Access Control Lists (IPv6 ACLs)..... 712

show cam-acl-egress.....	712
show cam-acl.....	713
permit icmp.....	715
permit.....	715
ipv6 control-plane egress-filter.....	716
ipv6 access-list.....	717
cam-acl-egress.....	718
cam-acl.....	719

26 Intermediate System to Intermediate System (IS-IS)..... 721

adjacency-check.....	721
advertise.....	722
area-password.....	723
clear config.....	724
clear isis.....	724
clns host.....	725
debug isis.....	726
debug isis adj-packets.....	726
debug isis local-updates.....	727
debug isis snp-packets.....	728
debug isis spf-triggers.....	729
debug isis update-packets.....	730
default-information originate.....	730
description.....	732
distance.....	732
distribute-list in.....	733
distribute-list out.....	734
distribute-list redistributed-override.....	735
domain-password.....	736
graceful-restart ietf.....	736
graceful-restart interval.....	737

graceful-restart restart-wait.....	738
graceful-restart t1.....	739
graceful-restart t2.....	739
graceful-restart t3.....	740
hello padding.....	741
hostname dynamic.....	742
ignore-lsp-errors.....	742
ip router isis.....	743
ipv6 router isis.....	744
isis circuit-type.....	745
isis csnp-interval.....	745
isis hello-interval.....	746
isis hello-multiplier.....	747
isis hello padding.....	748
isis ipv6 metric.....	748
isis metric.....	749
isis network point-to-point.....	750
isis password.....	751
isis priority.....	752
is-type.....	753
log-adjacency-changes.....	753
lsp-gen-interval.....	754
lsp-mtu.....	755
lsp-refresh-interval.....	756
max-area-addresses.....	757
max-lsp-lifetime.....	757
maximum-paths.....	758
metric-style.....	759
multi-topology.....	760
net.....	761
passive-interface.....	761
redistribute.....	762
redistribute bgp.....	764
redistribute ospf.....	765
router isis.....	766
set-overload-bit.....	767
show config.....	768
show isis database.....	769
show isis graceful-restart detail.....	772
show isis hostname.....	773
show isis interface.....	774
show isis neighbors.....	775
show isis protocol.....	777
show isis traffic.....	778
spf-interval.....	779



27 Link Aggregation Control Protocol (LACP).....	781
clear lacp counters.....	781
debug lacp.....	782
lacp long-timeout.....	783
lacp port-priority.....	784
lacp system-priority.....	784
port-channel-protocol lacp.....	785
show lacp.....	786
28 Layer 2.....	788
MAC Addressing Commands.....	788
mac-address-table aging-time.....	788
mac-address-table static.....	789
mac-address-table station-move refresh-arp.....	790
mac learning-limit.....	791
mac learning-limit learn-limit-violation.....	792
mac learning-limit mac-address-sticky.....	793
mac learning-limit station-move-violation.....	794
mac learning-limit reset.....	795
show mac-address-table.....	795
show mac-address-table aging-time.....	798
show mac learning-limit.....	798
Virtual LAN (VLAN) Commands.....	800
default vlan-id.....	800
description.....	801
default-vlan disable.....	801
name.....	802
show config.....	802
show vlan.....	803
tagged.....	806
track ip.....	807
untagged.....	808
Far-End Failure Detection (FEFD).....	809
debug fefd.....	810
fefd.....	810
fefd disable.....	811
fefd interval.....	812
fefd mode.....	813
fefd reset.....	814
fefd-global interval.....	814
fefd-global.....	815
show fefd.....	816
29 Link Layer Discovery Protocol (LLDP).....	818
LLPD Commands.....	818

advertise dot1-tlv.....	818
advertise dot3-tlv.....	819
clear lldp counters.....	820
clear lldp neighbors.....	821
debug lldp interface.....	821
disable.....	822
hello.....	823
mode.....	824
multiplier.....	825
protocol lldp (Configuration).....	825
protocol lldp (Interface).....	826
show lldp neighbors.....	827
show lldp statistics.....	828
LLDP-MED Commands.....	828
advertise med guest-voice.....	829
advertise med guest-voice-signaling.....	830
advertise med location-identification.....	831
advertise med power-via-mdi.....	832
advertise med softphone-voice.....	832
advertise med streaming-video.....	833
advertise med video-conferencing.....	834
advertise med video-signaling.....	835
advertise med voice.....	836
advertise med voice-signaling.....	837

30 Microsoft Network Load Balancing..... 838

arp (for Multicast MAC Address).....	838
mac-address-table static (for Multicast MAC Address).....	839
ip vlan-flooding.....	840

31 Multicast Source Discovery Protocol (MSDP)..... 841

clear ip msdp peer.....	841
clear ip msdp sa-cache.....	842
clear ip msdp statistic.....	842
ip msdp cache-rejected-sa.....	843
ip msdp default-peer.....	844
ip msdp log-adjacency-changes.....	845
ip msdp mesh-group.....	845
ip msdp originator-id.....	846
ip msdp peer.....	847
ip msdp redistribute.....	848
ip msdp sa-filter.....	849
ip msdp sa-limit.....	850
ip msdp shutdown.....	851
ip multicast-msdp.....	851
show ip msdp.....	852



show ip msdp sa-cache rejected-sa.....	853

32 Multiple Spanning Tree Protocol (MSTP).....855

debug spanning-tree mstp.....	855
disable.....	856
forward-delay.....	857
hello-time.....	858
max-age.....	858
msti.....	859
name.....	860
protocol spanning-tree mstp.....	861
revision.....	862
show config.....	863
show spanning-tree mst configuration.....	864
show spanning-tree msti.....	864
spanning-tree.....	867
spanning-tree msti.....	868
tc-flush-standard.....	869

33 Multicast.....870

IPv4 Multicast Commands.....	870
clear ip mroute.....	870
ip mroute.....	871
ip multicast-limit.....	872
ip multicast-routing.....	873
show ip mroute.....	874
show ip rpf.....	876

34 Neighbor Discovery Protocol (NDP).....878

IPv6 Router Advertisement (RA) Guard.....	878
clear ipv6 neighbors.....	879
debug ipv6 nd ra-guard.....	879
device-role.....	880
hop-limit.....	881
ipv6 nd ra-guard attach-policy.....	881
ipv6 nd ra-guard enable.....	882
ipv6 nd ra-guard policy.....	882
ipv6 neighbor.....	883
managed-config-flag.....	884
match ra.....	884
match ra.....	885
mtu.....	885
other-config-flag.....	886
reachable-time.....	887
retrans-time.....	887
router-lifetime.....	888

router-preference maximum.....	888
show config.....	889
show ipv6 nd ra-guard policy.....	890
show ipv6 neighbors.....	891
trusted-port.....	892

35 Object Tracking..... 893

IPv4 Object Tracking Commands.....	893
debug track.....	893
delay.....	894
description.....	895
show running-config track.....	895
show track.....	896
threshold metric.....	898
track interface ip routing.....	899
track interface line-protocol.....	900
track ip route metric threshold.....	900
track ip route reachability.....	901
track resolution ip route.....	902
IPv6 Object Tracking Commands.....	903
show track ipv6 route.....	904
track interface ipv6 routing.....	905
track ipv6 route metric threshold.....	906
track ipv6 route reachability.....	907
track resolution ipv6 route.....	908

36 Open Shortest Path First (OSPFv2 and OSPFv3)..... 910

OSPFv2 Commands.....	910
area default-cost.....	910
area nssa.....	911
area range.....	912
area stub.....	913
auto-cost.....	914
clear ip ospf.....	914
clear ip ospf statistics.....	915
debug ip ospf.....	916
default-information originate.....	918
default-metric.....	919
description.....	920
distance.....	921
distance ospf.....	921
distribute-list in.....	922
distribute-list out.....	923
fast-convergence.....	924
flood-2328.....	925
graceful-restart grace-period.....	926



graceful-restart helper-reject.....	927
graceful-restart mode.....	928
graceful-restart role.....	928
ip ospf auth-change-wait-time.....	929
ip ospf authentication-key.....	930
ip ospf cost.....	930
ip ospf dead-interval.....	931
ip ospf hello-interval.....	932
ip ospf message-digest-key.....	933
ip ospf mtu-ignore.....	934
ip ospf network.....	934
ip ospf priority.....	935
ip ospf retransmit-interval.....	936
ip ospf transmit-delay.....	937
log-adjacency-changes.....	937
maximum-paths.....	938
mib-binding.....	939
network area.....	939
passive-interface.....	940
redistribute.....	942
redistribute bgp.....	943
redistribute isis.....	944
router-id.....	945
router ospf.....	946
show config.....	947
show ip ospf.....	948
show ip ospf asbr.....	949
show ip ospf database.....	950
show ip ospf database asbr-summary.....	952
show ip ospf database external.....	954
show ip ospf database network.....	956
show ip ospf database nssa-external.....	958
show ip ospf database opaque-area.....	959
show ip ospf database opaque-as.....	960
show ip ospf database opaque-link.....	961
show ip ospf database router.....	962
show ip ospf database summary.....	965
show ip ospf interface.....	967
show ip ospf neighbor.....	969
show ip ospf routes.....	970
show ip ospf statistics.....	971
show ip ospf timers rate-limit.....	974
show ip ospf topology.....	975
summary-address.....	976
timers spf.....	977

timers throttle lsa all.....	978
timers throttle lsa arrival.....	979
OSPFv3 Commands.....	979
area authentication.....	979
area encryption.....	981
clear ipv6 ospf process.....	982
debug ipv6 ospf bfd.....	983
debug ipv6 ospf packet.....	984
default-information originate.....	986
graceful-restart grace-period.....	987
graceful-restart mode.....	987
ipv6 ospf area.....	988
ipv6 ospf authentication.....	989
ipv6 ospf cost.....	990
ipv6 ospf dead-interval.....	991
ipv6 ospf encryption.....	991
ipv6 ospf graceful-restart helper-reject.....	993
ipv6 ospf hello-interval.....	993
ipv6 ospf priority.....	994
ipv6 router ospf.....	995
maximum-paths.....	995
max-metric router-lsa.....	996
passive-interface.....	998
redistribute.....	999
router-id.....	1000
show crypto ipsec policy.....	1001
show crypto ipsec sa ipv6.....	1002
show ipv6 ospf database.....	1004
show ipv6 ospf interface.....	1006
show ipv6 ospf neighbor.....	1007
timers spf.....	1008

37 Policy-based Routing (PBR)..... 1010

description.....	1010
ip redirect-group.....	1011
ip redirect-list.....	1011
permit.....	1012
redirect.....	1013
seq.....	1015
show cam pbr.....	1017
show ip redirect-list.....	1017

38 PIM-Sparse Mode (PIM-SM)..... 1019

IPv4 PIM-Sparse Mode Commands.....	1019
clear ip pim rp-mapping.....	1019
clear ip pim tib.....	1020



debug ip pim.....	1021
ip pim bsr-border.....	1022
ip pim bsr-candidate.....	1022
ip pim dr-priority.....	1023
ip pim join-filter.....	1024
ip pim neighbor-filter.....	1025
ip pim query-interval.....	1026
ip pim register-filter.....	1026
ip pim rp-address.....	1027
ip pim rp-candidate.....	1028
ip pim sparse-mode.....	1029
ip pim sparse-mode sg-expiry-timer.....	1030
ip pim ssm-range.....	1031
ip pim spt-threshold.....	1032
show ip pim bsr-router.....	1033
show ip pim interface.....	1033
show ip pim neighbor.....	1035
show ip pim rp.....	1036
show ip pim ssm-range.....	1037
show ip pim summary.....	1037
show ip pim tib.....	1039

39 Port Monitoring..... 1041

description.....	1041
monitor multicast-queue.....	1042
monitor session.....	1043
rate-limit.....	1044
show config.....	1045
show monitor session.....	1045
show running-config monitor session.....	1046
source (port monitoring).....	1047

40 Private VLAN (PVLAN)..... 1050

ip local-proxy-arp.....	1051
private-vlan mode.....	1052
private-vlan mapping secondary-vlan.....	1053
switchport mode private-vlan.....	1054

41 Per-VLAN Spanning Tree Plus (PVST+)..... 1056

description.....	1056
disable.....	1057
extend system-id.....	1057
protocol spanning-tree pvst.....	1058
show spanning-tree pvst.....	1059
spanning-tree pvst.....	1062
spanning-tree pvst err-disable.....	1064

tc-flush-standard.....	1065
vlan bridge-priority.....	1066
vlan forward-delay.....	1067
vlan hello-time.....	1068
vlan max-age.....	1069

42 Quality of Service (QoS)..... 1071

Global Configuration Commands.....	1071
qos-rate-adjust.....	1071
service-class bandwidth-percentage.....	1072
service-class dot1p-mapping.....	1072
show qos dot1p-queue-mapping.....	1073
strict-priority queue.....	1073
Per-Port QoS Commands.....	1074
dot1p-priority.....	1074
rate police.....	1075
rate shape.....	1076
service-class dynamic dot1p.....	1077
Policy-Based QoS Commands.....	1078
bandwidth-percentage.....	1078
buffer-stats-snapshot.....	1079
class-map.....	1079
clear qos statistics.....	1081
description.....	1081
match ip access-group.....	1082
match ip dscp.....	1083
match ip precedence.....	1084
match mac access-group.....	1085
match mac dot1p.....	1086
match mac vlan.....	1086
policy-aggregate.....	1087
policy-map-input.....	1088
policy-map-output.....	1089
qos-policy-input.....	1089
qos-policy-output.....	1090
rate-police.....	1091
rate-shape.....	1092
service-policy input.....	1093
service-policy output.....	1093
service-queue.....	1094
set.....	1095
show qos class-map.....	1096
show qos policy-map.....	1096
show qos policy-map-input.....	1098
show qos policy-map-output.....	1099
show qos qos-policy-input.....	1099



show qos qos-policy-output.....	1100
show qos statistics.....	1101
show qos wred-profile.....	1102
service-class buffer shared-threshold-weight.....	1102
test cam-usage.....	1104
threshold.....	1105
trust.....	1106
wred.....	1107
wred ecn.....	1108
wred weight.....	1109
wred-profile.....	1110
rate shape.....	1111
service-pool wred.....	1112
DSCP Color Map Commands.....	1114
dscp.....	1114
qos dscp-color-map.....	1115
qos dscp-color-policy.....	1115
show qos dscp-color-policy	1116
show qos dscp-color-map	1117

43 Routing Information Protocol (RIP).....1119

auto-summary.....	1119
clear ip rip.....	1120
debug ip rip.....	1120
default-information originate.....	1121
default-metric.....	1122
description.....	1123
distance.....	1124
distribute-list in.....	1124
distribute-list out.....	1125
ip poison-reverse.....	1127
ip rip receive version.....	1127
ip rip send version.....	1128
ip split-horizon.....	1129
maximum-paths.....	1130
neighbor.....	1130
network.....	1131
offset-list.....	1132
output-delay.....	1133
passive-interface.....	1134
redistribute.....	1135
redistribute isis.....	1136
redistribute ospf.....	1137
router rip.....	1138
show config.....	1139
show ip rip database.....	1139

show running-config rip.....	1141
timers basic.....	1141
version.....	1142

44 Remote Monitoring (RMON)..... 1144

rmon alarm.....	1144
rmon collection history.....	1146
rmon collection statistics.....	1147
rmon event.....	1147
rmon hc-alarm.....	1148
show rmon.....	1150
show rmon alarms.....	1150
show rmon events.....	1152
show rmon hc-alarm.....	1153
show rmon history.....	1154
show rmon log.....	1155
show rmon statistics.....	1156

45 Rapid Spanning Tree Protocol (RSTP)..... 1159

bridge-priority.....	1159
debug spanning-tree rstp.....	1160
description.....	1161
disable.....	1161
forward-delay.....	1162
hello-time.....	1163
max-age.....	1164
protocol spanning-tree rstp.....	1164
show config.....	1165
show spanning-tree rstp.....	1166
spanning-tree rstp.....	1168
tc-flush-standard.....	1170

46 Security..... 1171

AAA Accounting Commands.....	1171
aaa accounting.....	1171
aaa accounting suppress.....	1173
accounting.....	1174
aaa radius group.....	1174
show accounting.....	1175
Authorization and Privilege Commands.....	1176
authorization.....	1176
aaa authorization commands.....	1177
aaa authorization config-commands.....	1178
aaa authorization exec.....	1178
privilege level (CONFIGURATION mode).....	1179
privilege level (LINE mode).....	1180



Obscure Password Commands.....	1181
service obscure-passwords.....	1181
Authentication and Password Commands.....	1182
aaa authentication enable.....	1182
aaa authentication login.....	1183
access-class.....	1185
enable password.....	1186
enable restricted.....	1187
enable secret.....	1188
login authentication.....	1189
password.....	1190
password-attributes.....	1191
service password-encryption.....	1192
show privilege.....	1193
show users.....	1194
timeout login response.....	1195
username.....	1196
RADIUS Commands.....	1197
debug radius.....	1197
ip radius source-interface.....	1198
radius-server deadtime.....	1199
radius-server group.....	1199
radius-server host.....	1200
radius-server vrf.....	1202
radius-server key.....	1203
radius-server retransmit.....	1204
radius-server timeout.....	1205
TACACS+ Commands.....	1205
tacacs-server group.....	1205
debug tacacs+.....	1206
ip tacacs source-interface.....	1207
tacacs-server group.....	1208
tacacs-server host.....	1208
tacacs-server key.....	1210
tacacs-server vrf.....	1211
Port Authentication (802.1X) Commands.....	1212
dot1x authentication (Configuration).....	1212
dot1x authentication (Interface).....	1213
dot1x auth-fail-vlan.....	1213
dot1x auth-server.....	1214
dot1x guest-vlan.....	1215
dot1x mac-auth-bypass.....	1216
dot1x max-eap-req.....	1216
dot1x port-control.....	1217
dot1x quiet-period.....	1217

dot1x reauthentication.....	1218
dot1x reauth-max.....	1219
dot1x server-timeout.....	1219
dot1x supplicant-timeout.....	1220
dot1x tx-period.....	1221
show dot1x interface.....	1221
SSH Server and SCP Commands.....	1223
crypto key generate.....	1223
crypto key zeroize rsa.....	1224
debug ip ssh.....	1224
ip scp topdir.....	1225
ip ssh authentication-retries.....	1226
ip ssh connection-rate-limit.....	1226
ip ssh hostbased-authentication.....	1227
ip ssh key-size.....	1228
ip ssh password-authentication.....	1229
ip ssh rekey	1229
ip ssh pub-key-file.....	1230
ip ssh rhostsfile.....	1231
ip ssh rsa-authentication (Config).....	1232
ip ssh server.....	1232
ip ssh server vrf.....	1235
ip ssh source-interface.....	1236
ip ssh vrf.....	1237
show crypto.....	1237
show ip ssh.....	1238
show ip ssh client-pub-keys.....	1239
show ip ssh rsa-authentication.....	1240
ssh.....	1241
Secure DHCP Commands.....	1243
clear ip dhcp snooping.....	1243
ip dhcp relay.....	1243
ip dhcp snooping.....	1244
ip dhcp snooping binding.....	1244
ip dhcp snooping database renew.....	1245
ip dhcp snooping trust.....	1246
ip dhcp source-address-validation.....	1246
ip dhcp snooping vlan.....	1247
show ip dhcp snooping.....	1247
Role-Based Access Control Commands.....	1248
aaa authorization role-only	1248
role	1249
show role	1250
show userroles	1251
userrole	1251



47 Service Provider Bridging.....	1253
debug protocol-tunnel.....	1253
protocol-tunnel.....	1254
protocol-tunnel destination-mac.....	1255
protocol-tunnel enable.....	1256
protocol-tunnel rate-limit.....	1256
show protocol-tunnel.....	1257
48 sFlow.....	1259
sflow collector.....	1259
sflow enable (Global).....	1261
sflow ingress-enable.....	1262
sflow extended-switch enable.....	1262
sflow max-header-size extended.....	1263
sflow polling-interval (Global).....	1264
sflow polling-interval (Interface).....	1265
sflow sample-rate (Global).....	1265
sflow sample-rate (Interface).....	1266
show sflow.....	1267
49 Simple Network Management Protocol (SNMP) and Syslog.....	1269
SNMP Commands.....	1269
show snmp.....	1269
show snmp engineID.....	1270
show snmp group.....	1271
show snmp user.....	1272
snmp ifmib ifalias long.....	1272
snmp-server community.....	1273
snmp-server contact.....	1275
snmp-server enable traps.....	1276
snmp-server engineID.....	1277
snmp-server group.....	1278
snmp-server host.....	1280
snmp-server location.....	1283
snmp-server packetsize.....	1283
snmp-server trap-source.....	1284
snmp-server user.....	1285
snmp-server user (for AES128-CFB Encryption).....	1287
snmp-server view.....	1288
snmp-server vrf.....	1289
snmp trap link-status.....	1290
Syslog Commands.....	1290
clear logging.....	1291
clear logging auditlog.....	1291
default logging buffered.....	1292

default logging console.....	1292
default logging monitor.....	1293
default logging trap.....	1293
logging.....	1294
logging buffered.....	1295
logging console.....	1296
logging extended.....	1297
logging facility.....	1298
logging history.....	1299
logging history size.....	1300
logging monitor.....	1301
logging on.....	1301
logging source-interface.....	1302
logging synchronous.....	1303
logging trap.....	1304
logging version.....	1305
show logging auditlog.....	1306
show logging.....	1306
show logging driverlog stack-unit.....	1308
terminal monitor.....	1308

50 SNMP Traps..... 1310

51 Storm Control..... 1315

show storm-control broadcast.....	1315
show storm-control multicast.....	1316
show storm-control unknown-unicast.....	1317
storm-control broadcast (Configuration).....	1318
storm-control broadcast (Interface).....	1319
storm-control multicast (Configuration).....	1320
storm-control multicast (Interface).....	1320
storm-control unknown-unicast (Configuration).....	1321
storm-control unknown-unicast (Interface).....	1322

52 Spanning Tree Protocol (STP)..... 1324

bridge-priority.....	1324
bpdu-destination-mac-address.....	1325
debug spanning-tree.....	1325
description.....	1326
disable.....	1327
forward-delay.....	1327
hello-time.....	1328
max-age.....	1329
protocol spanning-tree.....	1330
show config.....	1330
show spanning-tree 0.....	1331



spanning-tree.....	1334

53 System Time and Date..... 1337

clock summer-time date.....	1337
clock summer-time recurring.....	1338
clock timezone.....	1340
debug ntp.....	1340
ntp authenticate.....	1341
ntp broadcast client.....	1342
ntp disable.....	1343
ntp multicast client.....	1343
ntp master <stratum>.....	1344
ntp server.....	1344
ntp source.....	1346
ntp trusted-key.....	1346
ntp authentication-key.....	1347
show clock.....	1348
show ntp associations.....	1349
show ntp vrf associations.....	1350
show ntp status.....	1351

54 Tunneling 1353

ip unnumbered.....	1353
ipv6 unnumbered.....	1354
tunnel allow-remote.....	1354
tunnel destination.....	1355
tunnel dscp.....	1356
tunnel flow-label.....	1356
tunnel hop-limit.....	1357
tunnel keepalive.....	1357
tunnel-mode.....	1358
tunnel source.....	1359

55 VLAN Stacking..... 1361

dei enable.....	1361
dei honor.....	1362
dei mark.....	1363
member.....	1363
stack-unit stack-group.....	1364
vlan-stack access.....	1365
vlan-stack compatible.....	1365
vlan-stack dot1p-mapping.....	1367
vlan-stack protocol-type.....	1367
vlan-stack trunk.....	1368

56 Virtual Routing and Forwarding (VRF)..... 1371

ip unknown-unicast.....	1371
ipv6 unknown-unicast.....	1371
description.....	1372
ip vrf forwarding.....	1372
ip http vrf.....	1374
ip route-export.....	1374
ip route-import.....	1375
ipv6 route-export.....	1376
ipv6 route-import.....	1377
match source-protocol.....	1377
redistribute.....	1378
interface management.....	1379
maximum dynamic-routes.....	1379
show ip vrf.....	1380
show run vrf.....	1381

57 VLT Proxy Gateway.....1382

proxy-gateway lldp.....	1382
proxy-gateway static.....	1382
remote-mac-address exclude-vlan.....	1383
peer-domain-link port-channel exclude-vlan.....	1384
proxy-gateway peer-timeout	1384
vlt-peer-mac transmit.....	1385
show vlt-proxy-gateway.....	1385

58 Virtual Link Trunking (VLT).....1387

back-up destination.....	1387
clear vlt statistics.....	1388
delay-restore.....	1389
delay-restore abort-threshold.....	1390
lACP ungroup member-independent.....	1390
multicast peer-routing timeout.....	1391
peer-link port-channel.....	1392
peer-routing.....	1393
peer-routing-timeout.....	1393
primary-priority.....	1394
show vlt brief.....	1394
show vlt backup-link.....	1395
show vlt counters.....	1396
show vlt detail.....	1397
show vlt inconsistency.....	1398
show vlt mismatch.....	1399
show vlt role.....	1400
show vlt statistics.....	1401
show vlt statistics igmp-snoop.....	1403
unit-id.....	1403



vlt domain.....	1404
vlt-peer-lag port-channel.....	1405

59 Virtual Extensible LAN (VXLAN).....1406

feature vxlan.....	1406
debug vxlan.....	1406
fail-mode.....	1407
vxlan-instance.....	1407
vxlan-instance (VAP).....	1408
max_backoff.....	1408
gateway-ip.....	1409
controller.....	1409
show vxlan vxlan-instance.....	1410
show running-config vxlan.....	1411
show vxlan vxlan-instance unicast-mac-remote.....	1411
show vxlan vxlan-instance unicast-mac-local.....	1412
show vxlan vxlan-instance statistics interface.....	1413
show vxlan vxlan-instance physical-locator.....	1414
show vxlan vxlan-instance logical network.....	1414
clear vxlan vxlan-instance statistics.....	1415
clear mac-address-table dynamic all.....	1415

60 Virtual Router Redundancy Protocol (VRRP)..... 1417

IPv4 VRRP Commands.....	1417
advertise-interval.....	1417
authentication-type.....	1418
clear counters vrrp.....	1418
debug vrrp.....	1419
description.....	1420
disable.....	1421
hold-time.....	1421
preempt.....	1422
priority.....	1423
show config.....	1424
show vrrp.....	1424
track.....	1427
virtual-address.....	1428
vrrp delay minimum.....	1429
vrrp delay reload.....	1430
vrrp-group.....	1430
version.....	1431
IPv6 VRRP Commands.....	1432
clear counters vrrp ipv6.....	1432
debug vrrp ipv6.....	1433
show vrrp ipv6.....	1434
vrrp-ipv6-group.....	1436

About this Guide

This book provides information about the Dell Networking OS command line interface (CLI).

This book also includes information about the protocols and features found in Dell Networking OS.

References

For more information about your system, refer to the following documents:

- *Dell Networking OS Configuration Guides*
- *Installation and Maintenance Guides*
- *Release Notes*

Objectives

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



NOTE: For more information about when to use the CLI commands, refer to the *Dell Networking OS 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 font and must be entered in the CLI as listed.
<i>parameter</i>	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.

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.

Accessing the Command Line

When the system boots successfully, you are positioned on the command line in EXEC mode and not prompted to log in. You can access the commands through a serial console port or a Telnet session. When you Telnet into the 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, refer to the [Command Modes](#) section.

Multiple Configuration Users

When a user enters CONFIGURATION mode and another user is already in CONFIGURATION mode, the Dell Networking operating software 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)#ip ?
access-list      Named access-list
as-path          BGP autonomous system path filter
community-list   Add a community list entry
domain-list      Domain name to complete unqualified host name
domain-lookup    Enable IP Domain Name System hostname translation
domain-name      Define the default domain name
fib              FIB configuration commands
ftp              FTP configuration commands
host             Add an entry to the ip hostname table
max-frag-count   Max. fragmented packets allowed in IP re-assembly
multicast-routing Enable IP multicast forwarding
name-server      Specify address of name server to use
pim Protocol     Independent Multicast
prefix-list      Build a prefix list
radius           Interface configuration for RADIUS
redirect-list    Named redirect-list
route            Establish static routes
scp              SCP configuration commands
source-route     Process packets with source routing header options
ssh              SSH configuration commands
tacacs           Interface configuration for TACACS+
telnet           Specify telnet options
tftp             TFTP configuration commands
trace-group      Named trace-list
trace-list       Named trace-list
Dell(conf)#ip
```

When entering commands, you can take advantage of the following timesaving features:

- The commands are not case-sensitive.
- You can enter partial (truncated) command keywords. For example, you can enter `int teng 1/1` for the interface `tengigabitethernet 1/1` 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 Dell Networking OS command line, use the left and right Arrow keys.

The shortcut key combinations at the Dell Networking OS command line are as follows:

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

Dell Networking OS 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, refer to 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. In this guide, 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`

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 TenGigabitEthernet 1/1/1

```
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.`

Enabling Software Features on Devices Using a Command Option

This capability to activate software applications or components on a device using a command is supported on the S4810, S4820T, and S6000, platforms.

Starting with Release 9.4(0.0), you can enable or disable specific software functionalities or applications that need to run on a device by using a command attribute in the CLI interface. This capability enables effective, streamlined management and administration of applications and utilities that run on a device. You can employ this capability to perform an on-demand activation or turn-off of a software component or protocol. A feature configuration file that is generated for each image contains feature names denotes whether this enabling or disabling method is available for such features. In 9.4(0.0), you can enable or disable the VRF application globally across the system by using this capability.

You can activate VRF application on a device by using the `feature vrf` command in CONFIGURATION mode.

 **NOTE: The `no feature vrf` command is not supported on any of the platforms.**

To enable the VRF feature and cause all VRF-related commands to be available or viewable in the CLI interface, use the following command. You must enable the VRF feature before you can configure its related attributes.

```
Dell(conf)# feature vrf
```

Based on whether VRF feature is identified as supported in the Feature Configuration file, configuration command `feature vrf` becomes available for usage. This command will be stored in running-configuration and will precede all other VRF-related configurations.

 **NOTE: The MXL and Z9000 platforms currently do not support VRF. These platforms support only the management and default VRFs, which are available by default. As a result, the `feature vrf` command is not available for these platforms.**

To display the state of Dell Networking OS features:

```
Dell#show feature
```

Example of show feature output

For a particular target where VRF is enabled, the show output is similar to the following:

```
Feature State
-----
VRF          enabled
```

feature vrf

Enable the VRF application on a switch. After you enable the VRF feature, you cannot deactivate it.

Syntax	<code>feature vrf</code>	
Defaults	Disabled	
Command Modes	CONFIGURATION	
Command History	Version 9.5(0.0)	Introduced on the Z9500.
	Version 9.4(0.0)	Introduced on the S4810, S4820T, S5000, and S6000.
Usage Information	You can activate VRF application on a device by using the <code>feature vrf</code> command in CONFIGURATION mode. The <code>no feature vrf</code> command is not supported on any platform.	



show feature

Verify the status of software applications, such as VRF, that are activated and running on a device.

Syntax	<code>show feature</code>	
Command Modes	EXEC	
	EXEC Privilege	
Command History	Version 9.4(0.0)	Introduced on the S4810, S4820T, and S6000.
Usage Information	You can activate VRF application on a device by using the <code>feature vrf</code> command in CONFIGURATION mode. The <code>no feature vrf</code> command is not supported on any of the platforms.	
Example	<pre>Dell#show feature Feature State ----- VRF enabled</pre>	

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 for BGP, use BGP ADDRESS-FAMILY mode. For more information, refer to [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`
3. Enter the protocol type.
 - For IPv4, enter `ipv4 multicast`. The prompt changes to include (conf-router_bgp_af) for IPv4.

CLASS-MAP Mode

To create or configure a class map, use CLASS-MAP mode. For more information, refer to [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.

CONTROL-PLANE Mode

To manage control-plane traffic, use CONTROL-PLANE mode. For more information, refer to [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, refer to [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, refer to [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, refer to [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.

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.

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, refer to [Force10 Resilient Ring Protocol \(FRRP\)](#).

To enter FRRP mode:

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

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

INTERFACE Mode

Use INTERFACE mode to configure interfaces or IP services on those interfaces. An interface can be physical (for example, a 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[/subport] number. For example:

Prompt	Interface Type
Dell (conf-if) #	INTERFACE mode

Prompt	Interface Type
Dell (conf-if-te-1/1) #	Ten-Gigabit Ethernet interface then slot/port/ <i>subport</i> information
Dell (conf-if-fo-1/1) #	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-po-0) #	Port-channel interface number
Dell (conf-if-vl-0) #	VLAN Interface then VLAN number (range 1–4094)
Dell (conf-if-ma-1/1) #	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.

ISIS ADDRESS-FAMILY Mode

To enable or configure IPv6 for ISIS, use ISIS ADDRESS-FAMILY mode. For more information, refer to [Intermediate System to Intermediate System \(IS-IS\)](#).

To enter ISIS ADDRESS-FAMILY mode:

1. Verify that you are logged in to ROUTER ISIS mode.
2. Enter the command `address-family ipv6 unicast`. The prompt changes to include (conf-router_isis-af_ipv6).

LLDP Mode

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

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, refer to [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, refer to [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.

OPENFLOW INSTANCE Mode

To enable and configure OpenFlow instances, use OPENFLOW INSTANCE mode.

To enter OPENFLOW INSTANCE mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `openflow of-instance` command then the OpenFlow ID number of the instance you want to create or configure. The prompt changes to include (conf-of-instance *of-id*).

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

Per-VLAN SPANNING TREE (PVST+) Plus Mode

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

PROTOCOL GVRP Mode

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

RAPID SPANNING TREE (RSTP) Mode

To enable and configure RSTP, use RSTP mode. For more information, refer to [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, refer to [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 ISIS Mode

To enable and configure Intermediate System to Intermediate System (ISIS), use ROUTER ISIS mode. For more information, refer to [Intermediate System to Intermediate System \(IS-IS\)](#).

To enter ROUTER ISIS mode:

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

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

ROUTER OSPF Mode

To configure OSPF, use ROUTER OSPF mode. For more information, refer to [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.

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, refer to [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, refer to [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.

VLT DOMAIN Mode

To enable and configure the VLT domain protocol, use VLT DOMAIN mode. For more information, refer to [Virtual Link Trunking \(VLT\)](#).

To enter VLT DOMAIN mode:

1. Verify that you are logged in to CONFIGURATION mode.
2. Enter the `vlt domain` command then the VLT domain number. The prompt changes to include (conf-vlt-domain).

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

VRRP Mode

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



File Management

This chapter contains command line interface (CLI) commands needed to manage the configuration files as well as other file management commands.

boot system

Tell the system where to access the Dell Networking OS image used to boot the system.

Syntax

```
boot system {gateway ip address| stack-unit [{stack-unit-number | all}
[default | primary {system {A: | B: | bmp-boot} | tftp: | | secondary}]}
```

To return to the default boot sequence, use the `no boot system` command.

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.
stack-unit	Enter the stack-unit number for the master switch.
stack-unit-number	Enter the stack-unit number. The range is from 1 to 6.
default	Enter the keyword <code>default</code> to use the primary Dell Networking OS image.
primary	Enter the keyword <code>primary</code> to use the primary Dell Networking OS image.
secondary	Enter the keyword <code>secondary</code> to use the primary Dell Networking OS image.
tftp:	Enter the keyword <code>TFTP:</code> to retrieve the image from an FTP server. <code>ftp://userid:password@hostip/filepath</code> .
nfsmount	Enter the keyword <code>nfsmount:</code> to retrieve the image from a mounted NFS file system. <code>nfsmount://filepath</code>
system:	Enter the keyword <code>system:</code> to retrieve the image from the system.
usbflash	Enter the keyword <code>usbflash:</code> to retrieve the image from the USB flash memory. <code>usbflash://filename</code> .
tftp:	Enter the keyword <code>TFTP:</code> to retrieve the image from a TFTP server. <code>tftp://hostip/filepath</code> .
A: B:	Enter <code>A:</code> or <code>B:</code> to boot one of the system partitions.
bmp-boot	Enter the keyword <code>bmp-boot</code> to boot the system, when the you are not sure about the partition that contains image from DHCP offer.



NOTE: In normal-reload, this keyword is not enabled.

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 the support for <code>bmp-boot</code> on the S-Series and Z-Series switches.
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 To display these changes in the `show bootvar` command output, save the running configuration to the startup configuration (using the `copy` command) and reload system.

The keyword `bmp-boot` is used only when the device boots up from BMP. In case of industrial standard upgraded device, the Dell networking OS stores the image partition upgraded from the DHCP offer in `bmp-boot` variable.

cd

Change to a different working directory.

Syntax `cd directory`

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:` (internal Flash) or any sub-directory

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
9.7(0.0)	Added NFS mount support. 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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

HTTP Copy via CLI

Copy one file to another location. Dell Networking OS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP (in the *hostip* field).

This feature is supported on platform.

Syntax `copy http://10.16.206.77/sample_file flash://sample_file`
`copy flash://sample_file http://10.16.206.77/sample_file`
 You can copy from the server to the switch and vice-versa.

Parameters

copy http: Address or name of remote host []: 10.16.206.77
flash: Port number of the server [80]:
 Source file name []: sample_file
 User name to login remote host: x
 Password to login remote host:
 Destination file name [sample_file]:

Defaults None.

Command Modes EXEC Privilege

Command History

Version	Description
9.3(0.1)	Introduced on the S6000, Z9000, S4810, and S4820T.

Example `copy http://admin:admin123@10.16.206.77/sample_file flash://sample_file`

Related Commands `copy ftp:flash`
 Copy files from FTP server to switch



copy

Copy one file to another location. Dell Networking OS supports IPv4 and IPv6 addressing for FTP, TFTP, and SCP (in the *hostip* field).

Syntax

```
copy compressed-config source-file-url destination-file-url
```

Parameters

Enter the following location keywords and information:

compressed-config	Enter the keyword <code>compressed-config</code> 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 <i>hostip</i> field).	
file-url	To copy a file from the internal FLASH	enter <code>flash://</code> followed by the filename
	To copy a file on an FTP server	enter <code>ftp://user:password@hostip/filepath</code>  NOTE: For FTP copy operations done through external servers, the password you specify for accessing the FTP server can be a string of up to 32 characters in length.
	To copy a file on a HTTP server	enter <code>http: http://hostip/filepath</code>  NOTE: For HTTP copy operations done through external servers, the password you specify for accessing the HTTP server can be a string of up to 32 characters in length.
	To copy a file on a NFS mounted system	enter <code>nfsmount://<mount-point/filepath</code>  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 <code>running-config</code>
	To copy the startup configuration	enter the keyword <code>startup-config</code>
	To copy using a Secure Copy (SCP),	enter the keyword <code>scp</code> : • If you enter <code>scp</code> in the source position, enter the target URL; • If you enter <code>scp</code> in the target position, first enter the source URL;  NOTE: For SCP copy operations done through external servers, the password you specify can be a string of up to 32 characters in length.



To copy a file on the external FLASH	enter <code>slot0://</code> followed by the filename
To copy a file on a TFTP server	enter <code>tftp://hostip/filepath</code>
To copy a file from an external USB drive	enter <code>usbflash://filepath</code>

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
9.7(0.0)	Introduced on the S6000-ON. Added the <code>nfsmount:<mount-point></code> parameters that enables you to mount a remote NFS file system.
9.4(0.0)	Added the <code>compressed-config</code> 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 <code>usbflash</code> and <code>rpm0usbflash</code> 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 (the startup configuration file amended by any configuration changes made since the system was started) to the startup configuration file, Dell Networking OS creates a backup file on the internal flash of the startup 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 are enhanced to display and store the running configuration in the compressed mode.

Example

```
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
```

In this `copy scp: flash:` example, specifying 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.

Example

```
Dell#copy running-config nfsmount://<mount-point>/filepath
Destination file name [test.txt]:
User name to login remote host: username
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
FTOS#
FTOS#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
```

Related Commands [cd](#) – changes the working directory.

delete

Delete a file from the flash. After deletion, files cannot be restored.

Syntax `delete flash-url [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.

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, refer to the relevant *Dell 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. Added support for NFS mount.
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.

dir

Display the files in a file system. The default is the current directory.

Syntax

`dir [filename | directory name:]`

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.

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
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Added support for NFS mount.
8.3.19.0	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)
```

Related Commands [cd](#) – changes the working directory.



format (S-Series)

Erase all existing files and reformat the filesystem in the internal flash memory. After the filesystem is formatted, files cannot be restored.

Syntax `format {flash: | usbflash:}`

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series

Usage Information You must include the colon (:) when entering this command.

After reformatting is complete, three empty directories are automatically created on flash: CRASH_LOG_DIR, TRACE_LOG_DIR and NVTRACE_LOG_DIR.



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).

Related Commands [copy](#) – copies the current configuration to either the startup-configuration file or the terminal.

[show file-systems](#) – displays information about the file systems on the system.

fsck flash

Checks the flash file system for errors.

Syntax `fsck flash:`
`fsck usbflash:`

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
9.1(0.0)	Introduced on S4810 and Z9000.
8.3.19.0	Introduced on S4820T.

Usage Information Include the colon (:) when entering this command. This command checks the specified flash memory for errors. If errors are found, the command recommends that you format the flash.

 **CAUTION: If you elect to format the flash, all files – including the startup configuration file – are lost. If you do decide to format the specified flash, consider saving the running configuration as the startup configuration after formatting the flash (use the `write memory` command or `copy run start` command).**

Related Commands

- [copy](#) — copy one file to another location.
- [show file-systems](#) — Display information about the file systems on the system.

mkdir

Creates a directory on the NFS mounted file system.

Syntax `mkdir nfsmount://mount-point/username`

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 S-Series.

Example `Dell#mkdir nfsmount:/nfs-mountpoint/guest`

Related Commands [rmdir](#) – removes a directory.



mount nfs

Mounts an NFS file system to a device.

Syntax `mount nfs rhost:path mount-point [username password]`

Parameters Enter the following location keywords and information:

<i>rhost:path</i>	Enter the remote hosts's path directory.
<i>mount-point</i>	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
9.7(0.0)	Introduced on the S-Series.

Example `Dell#mount nfs nfstest nfs-mount-point username pwd`

Related Commands [cd](#) – changes the working directory.

rmdir

Removes a directory from the NFS mounted file system.

Syntax `rmdir nfsmount://mount-point/username`

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 S-Series.

Example `Dell#rmdir nfsmount:/nfs-mountpoint/guest
Proceed to remove the directory [confirm yes/no]: yes
Dell#`

Related Commands [mkdir](#) – creates a directory.



upgrade system

Upgrade the Dell Networking OS image. To upgrade the bootflash or bootselector image, use the `upgrade boot` command.

Syntax	<code>upgrade system {flash: ftp: nfsmount: scp: stack-unit {stack-unit-id all}}</code>	
Parameters	system	Enter the keyword <code>system</code> to upgrade the operating system (OS) image.
	flash: file-url	Enter the keyword <code>flash:</code> and specify the location of the image file in the format <code>//director</code>
	ftp: file-url	Enter the keyword <code>ftp:</code> and specify the location of the image file in the format <code>//userid:pas</code>
	nfsmount://<mount-point>/filepath	Enter the keyword <code>nfsmount:</code> and specify the location of the image file in the format <code>//<mount</code>
	scp: file-url	Enter the keyword <code>scp:</code> and specify the location of the image file in the format <code>userid:passw</code>
	stack-unit stack-unit-id	Enter the keyword <code>stack-unit</code> and specify the stack-unit ID to sync the image to that stack-un
	stack-unit all	Enter the keyword <code>stack-unit</code> followed by the keyword <code>all</code> to sync the image on all stack-un
	tftp: file-url	Enter the keyword <code>tftp:</code> and specify the location of the image file in the format <code>//host-ip/f</code>
	usbflash: file-url	Enter the keyword <code>usbflash:</code> and specify the location of the source file in the format <code>//direc</code>
	A: B:	Specify the flash partition of the operating-system image to be upgraded.

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

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 <code>file-url</code> 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 RFC 3986 specifies that IPv6 host addresses in a uniform resource identifier (URI) must be enclosed in square brackets, [].
After you upgrade the system image, by entering the command. specify the location where the Dell Networking OS image



Example

```
Dell# upgrade system tftp://10.11.8.12/dv-rainier-13 a:
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
```

rename

Rename a file in the local file system.

Syntax `rename url url`

Parameters

url

Enter the following keywords and a filename:

- For a file on the internal Flash, enter `flash://` followed by the filename.
- For a file on an NFS mounted file system, enter `nfsmount://` followed by the mount point and file path.
- For a file on an external USB drive, enter `usbflash://` followed by the filename.

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
9.7(0.0)	Introduced on the S6000-ON. Added support for NFS mount.
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

show boot system

Displays information about boot images currently configured on the system.

Syntax `show boot system {stack-unit | all}`



Parameters

all

Enter the keyword `all` to display the boot image information for all stack units.

stack-unit

Enter the keyword `stack-unit` followed by a number to display boot image information for a stack-unit.
The range is from 1 to 6.

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
9.7(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.
7.7.1.0	Introduced on the C-Series and E-Series.

Example

Dell#show boot system stack-unit 1

Current system image information in the system:

=====

Type	Boot Type	A	B
Stack-unit 1	FLASH BOOT	9-0 (2-1)	9-0 (2-0) [boot]

Dell#

show bootvar

Display the variable settings for the boot parameters.

Syntax	<code>show bootvar</code>
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. 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.
9.0.2.0	Introduced on the S6000.
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.
E-Series	Original command.

Example

```
Dell#show bootvar
PRIMARY IMAGE FILE = system://B
SECONDARY IMAGE FILE = tftp://10.16.127.35/Dell-SI-9-0-2-0.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 = system://B
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 = 10.16.132.254
Reload Mode = normal-reload
Dell#
```

show file-systems

Display information about the file systems on the system.

Syntax `show file-systems`

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
9.7(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



Version	Description
E-Series	Original command

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#
```

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 <code>network</code> is listed.
Flags	Displays the access available to the storage location. The following letters indicate the level of access: • <code>r</code> = read access • <code>w</code> = write access
Prefixes	Displays the name of the storage location.

Related Commands

[format flash \(S-Series\)](#) – Erases all the existing files and reformats the filesystem in the internal flash memory on the S-Series.

show os-version

Display the release and software image version information of the image file specified.

Syntax `show os-version [file-url]`

Parameters

file-url	(OPTIONAL) Enter the following location keywords and information: • For a file on the internal flash, enter <code>flash://</code> followed by the filename. • For a file on an FTP server, enter <code>ftp://user:password@hostip/filepath</code>. • For a file on a TFTP server, enter <code>tftp://hostip/filepath</code>. • For a file on the USB port, enter <code>usbflash://filepath</code>.

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
9.7(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.

Usage Information



NOTE: A filepath that contains a dot (.) is not supported.

show running-config

Display the current configuration and display changes from the default values.

Syntax

```
show running-config [entity] [configured] [status] [compressed]
```

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
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
cam-profile	for the current CAM profile in the configuration
class-map	for the current class-map configuration
community-list	for the current community-list configuration
ecmp-group	for the current ECMP group configuration
eis	for the current EIS configuration

ethernet	for the current Ethernet CFM configuration
fefd	for the current FEFD configuration
ftp	for the current FTP configuration
frrp	for the current FRRP configuration
fvrp	for the current FVRP configuration
gvrp	for the current GVRP configuration
host	for the current host configuration
hardware-monitor	for hardware-monitor action-on-error settings
hypervisor	for the current hypervisor configuration
igmp	for the current IGMP configuration
interface	for the current interface configuration
interface port-channel	for the current port-channel interface configuration. The range is from 1 to 128.
interface tunnel	for all configured tunnels. For a specific tunnel, enter the tunnel ID. The range is from 1 to 16383.
ip	for the current IP configuration
isis	for the current ISIS configuration
line	for the current line configuration
lldp	for the current LLDP configuration
load-balance	for the current port-channel load-balance configuration
logging	for the current logging configuration
mac	for the current MAC ACL configuration
mac-address-table	for the current MAC 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
ospf	for the current OSPF 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-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
resolve	for the current DNS configuration
rip	for the current RIP configuration
rmon	for the current RMON configuration
route-map	for the current route map 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
trace-group	for the current trace-group configuration
trace-list	for the current trace-list configuration
uplink-state-group	for the uplink state group configuration
users	for the current users configuration
vlt	for the current VLT configuration
wred-profile	for the current wred-profile configuration

configured	(OPTIONAL) Enter the keyword <code>configuration</code> to display line card interfaces with non-default configurations only.
status	(OPTIONAL) Enter the keyword <code>status</code> to display the checksum for the running configuration and the start-up configuration.
compressed	(Optional) Enter the keyword <code>compressed</code> to display the compressed group configuration. Displays the compressed configuration by grouping all similar configurations. The compression is done only for interface related configurations.



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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
9.2.(0.0)	Added support for the tunnel and EIS interface types.
9.0.0.0	Added support for the VLT option.
8.3.19.0	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 hardware-monitor option.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Expanded to include the last configuration change, start-up last updated (date and time), and who made the change.
6.5.4.0	Added the status option.

Example

```
Dell# show running-config
Current Configuration ...
! Version 9-0(2-0)
! Last configuration change at Thu Apr 18 10:18:39 2013 by admin
! Startup-config last updated at Thu Apr 18 10:18:40 2013 by admin
!
boot system stack-unit 1 primary system: A:
boot system stack-unit 1 secondary tftp://10.16.127.35/Dell-SI-9-0-2-0.bin
boot system stack-unit 1 default system: A:
boot system gateway 10.16.132.254
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
!
redundancy disable-auto-reboot stack-unit 1
redundancy disable-auto-reboot stack-unit 2
redundancy disable-auto-reboot stack-unit 3
redundancy disable-auto-reboot stack-unit 4
redundancy disable-auto-reboot stack-unit 5
redundancy disable-auto-reboot stack-unit 6
!
hardware watchdog stack-unit 1
hardware watchdog stack-unit 2
hardware watchdog stack-unit 3
```

Example

```
Dell#show running-config status
running-config bytes 10257, checksum 0xFD33339F
startup-config bytes 10257, checksum 0xFD33339F
```

Usage Information The status option allows you to display the size and checksum of the running configuration and the startup configuration.



show startup-config

Display the startup configuration.

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
9.7(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 S-Series
7.5.1.0	Introduced on the C-Series.
7.4.1.0	Expanded to include the last configuration change, start-up last updated (date and time), and who made the change.

Example

```
Dell#show startup-config
! Version 9-0(2-0)
! Last configuration change at Thu Apr 18 10:18:39 2013 by admin
! Startup-config last updated at Thu Apr 18 10:18:40 2013 by admin
!
boot system stack-unit 0 primary system: A:
boot system stack-unit 0 secondary tftp://10.16.127.35/Dell-SI-9-0-2-0.bin
boot system stack-unit 0 default system: A:
boot system gateway 10.16.132.254
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
...
```

Related Commands [show running-config](#) – displays the current (running) configuration.

show version

Display the current Dell Networking Operating System (OS) version information on the system.

Syntax `show version`

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
9.7(0.0)	Introduced on the S6000-ON.
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.
7.6.1.0	Introduced on the S-Series
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

Command Fields

Lines Beginning With	Description
Dell Network...	Name of the operating system
Dell Operating...	OS version number
Dell 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 Networking OS uptime is...	Amount of time the system has been up
System image...	Image file name
System Type:	S4810, S4820T, Z9000, S6000
Control Processor:...	Control processor information and amount of memory on processor
128K bytes...	Amount and type of memory on system
1 Route Processor...	Hardware configuration of the system, including the number and type of physical interfaces available

Example (S-Series)

```

Dell#show version
Dell Real Time Operating System Software
Dell Operating System Version: 1.0
Dell Application Software Version: E7-8-1-13
Copyright (c) 1999-2008 by Dell Force10 Networks, Inc.
Build Time: Mon Nov 24 18:59:27 2008
Build Path: /sites/sjc/work/sw/build/build2/Release/E7-8-1/SW/SRC
Dell uptime is 1 minute(s)
System Type: S50V
Control Processor: MPC8451E with 252739584 bytes of memory.

32M bytes of boot flash memory.

  1 48-port E/FE/GE with POE (SB)
  48 GigabitEthernet/IEEE 802.3 interface(s)
  4 Ten GigabitEthernet/IEEE 802.3 interface(s)
Dell#

```



Example (S4810)

```
Dell#
Dell#show version
Dell Real Time Operating System Software
Dell Operating System Version: 1.0
Dell Application Software Version: Z9K-ICC-PRIM-SYNC-8-3-11-173
Copyright (c) 1999-2012 by Dell Inc. All Rights Reserved.
Build Time: Mon Jul 16 22:19:01 PDT 2012
Build Path: /local/local/build/build15/8.3.12.0/SW/SRC/Radius
Dell uptime is 1 minute(s)
System image file is "s4810-14"
System Type: S4810
Control Processor: Freescale QorIQ P2020 with 2147483648 bytes of memory.
128M bytes of boot flash memory.
1 52-port GE/TE/FG (SE)
52 Ten GigabitEthernet/IEEE 802.3 interface(s)
```

Example (S6000)

```
Dell#S6000#show version
Dell Real Time Operating System Software
Dell Operating System Version: 2.0
Dell Application Software Version: 9-4(0-119)
Copyright (c) 1999-2014 by Dell Inc. All Rights Reserved.
Build Time: Tue Mar 18 10:32:02 PDT 2014
Build Path: /work.local/build/buildSpaces/build01/E9-4-0/SW/SRCC
Dell Networking OS uptime is 1 day(s), 0 hour(s), 19 minute(s)
System image file is "DT-MAA-S6000-16-PI"
System Type: S6000
Control Processor: Intel Centerton with 3203911680 bytes of memory,
core(s) 2.
16G bytes of boot flash memory.
1 32-port TE/FG (SI)
32 Forty GigabitEthernet/IEEE 802.3 interface(s)
```

upgrade system

Upgrade the system image.

Syntax

```
upgrade system {flash: | ftp: | scp: | tftp: | usbflash: | stack-unit {0-5
| all} {A: | B:}}
```

Parameters

0-5	Enter the keywords 0-5 to upgrade only the mentioned stack-unit.
all	Enter the keyword all to upgrade all the member units of the stack.
ftp	Enter the keyword ftp to follow it with the location of the source file in this form: <i>//userid:password@hostip/filepath</i> , or press Enter to launch a prompt sequence.
scp	Enter the keyword scp to follow it with the location of the source file in this form: <i>//userid:password@hostip/filepath</i> , or press Enter to launch a prompt sequence.
tftp	Enter the keyword tftp to follow it with the location of the source file in this form: <i>//hostlocation/filepath</i> , or press Enter to launch a prompt sequence.
flash	Enter the keyword flash to follow it with the location of the source file in this form: <i>//filepath</i> , or press Enter to launch a prompt sequence.



usbflash	Enter the keyword <code>flash</code> to follow it with the location of the source file in this form: <code>//filepath</code> , or press Enter to launch a prompt sequence.
A	Enter the keyword <code>A</code> to upgrade the bootflash partition A
B	Enter the keyword <code>B</code> to upgrade the bootflash partition B.

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 9.0.2.0	Introduced on the S6000.
Version 9.0(0.0)	Added support for IPv6 for the <code>file-url</code> parameter.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000. Added support for the SSD on the Z9000 only.
Version 8.3.7.0	Introduced on the S4810.

Usage Information You must reload FTOS after executing this command. Use the command `upgrade system stack-unit` to copy FTOS from the management unit to one or more stack members.

Example

```
Dell#upgrade system ?
flash: Copy from flash file system (flash://filepath)
ftp: Copy from remote file system, IPv4 or IPv6, (ftp://
userid:password@hostip/filepath)
scp: Copy from remote file system, IPv4 or IPv6, (scp://
userid:password@hostip/filepath)
stack-unit Sync image to the stack-unit
tftp: Copy from remote file system, IPv4 or IPv6, (tftp://
hostip/filepath)
usbflash: Copy from usbflash file system (usbflash://filepath)
Dell#
```

upgrade boot

Upgrade the bootflash image or bootselector image.

Syntax `upgrade boot {all | bootflash-image | bootselector-image}stack-unit {0-5 | all}{booted | flash: | ftp: | scp: | tftp: | usbflash:} {A: | B:}`

Parameters

all	Enter the keyword <code>all</code> to change both the bootflash and bootselector images.
bootflash-image	Enter the keyword <code>bootflash-image</code> to change the bootflash image..
bootselector-image	Enter the keyword <code>bootselector-image</code> to upgrade the BIOS system image.
0-5	Enter the keywords <code>0-5</code> to upgrade only the mentioned stack-unit .



all	Enter the keywords <code>all</code> to upgrade the member stack-units.
booted	Enter the keyword <code>booted</code> to upgrade from the current image in the S6000.
ftp	Enter the keyword <code>ftp</code> to follow it with the location of the source file in this form: <code>//userid:password@hostip/filepath</code> , or press Enter to launch a prompt sequence.
tftp	Enter the keyword <code>tftp</code> to follow it with the location of the source file in this form: <code>//hostlocation/filepath</code> , or press Enter to launch a prompt sequence.
flash	Enter the keyword <code>flash</code> to follow it with the location of the source file in this form: <code>//filepath</code> , or press Enter to launch a prompt sequence.
usbflash	Enter the keyword <code>flash</code> to follow it with the location of the source file in this form: <code>//filepath</code> , or press Enter to launch a prompt sequence.
A	Enter the keyword <code>A</code> to upgrade the bootflash partition A
B	Enter the keyword <code>B</code> to upgrade the bootflash partition B.

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 9.0.2.0	Introduced on the S6000.
Version 9.0(0.0)	Added support for IPv6 for the <code>file-url</code> parameter.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.11.1	Introduced on the Z9000. Added support for the SSD on the Z9000 only.
Version 8.3.7.0	Introduced on the S4810.
Version 7.7.1.0	Added support for TFTP and SCP.
Version 7.6.1.0	Introduced on the S-Series.

Usage Information You must reload Dell Networking OS after executing this command.

Example

```
Dell#upgrade boot ?
all Upgrade both boot flash image and selector image
bootflash-image Upgrade boot flash image
bootselector-image Upgrade boot selector image
Dell#
```


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.

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 <code>flash://</code> 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.

Defaults flash drive

Command Modes EXEC mode

Command History Version 9.5.(0.0)

Version	Description
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:
e6328c06faf814e6899ceed219afbf9360e986d692988023b749e6b2093e933
```

Entering the Hash Value for Verification using SHA256

```
Dell# verify sha256 flash://FTOS-SE-9.5.0.0.bin
e6328c06faf814e6899ceed219afbf9360e986d692988023b749e6b2093e933
SHA256 hash VERIFIED for FTOS-SE-9.5.0.0.bin
```



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).

 **NOTE:** This command replaces the `enable optic-info-update interval` command to update information on temperature and power monitoring in the simple network management protocol (SNMP) management information base (MIB).

banner exec

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

Syntax	<code>banner exec c line c</code> To delete a banner, use the <code>no banner exec</code> command.	
Parameters	c	Enter the keywords <code>banner exec</code> , then enter a character delineator, represented here by the letter <code>c</code> . 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

Version	Description
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 banner EXEC (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 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.

Syntax `banner login {keyboard-interactive | no keyboard-interactive} [c line c]`
Enter **no banner login** to delete the banner text. Enter **no banner login keyboard-interactive** to automatically go to the banner message prompt (does not require a carriage return).

Parameters

keyboard-interactive	Enter the keyword <code>keyboard-interactive</code> to require a carriage return (CR) to get the message banner prompt.
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, refer to the relevant *Dell 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.
9.0.2.0	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.
8.2.1.0	Introduced the keyword <code>keyboard-interactive</code> .
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 banner EXEC (if configured) displays.

Example

```
Dell(conf)#banner login ?
keyboard-interactive Press enter key to get prompt
LINE c banner-text c, where 'c' is a delimiting character
Dell(conf)#no banner login ?
keyboard-interactive Prompt will be displayed by default
<cr>
Dell(conf)#banner login keyboard-interactive

Enter TEXT message. End with the character '%'.
This is the banner%
Dell(conf)#end
Dell#exit

13d21h9m: %RPM0-P:CP %SEC-5-LOGOUT: Exec session is terminated for user on
line console

This is the banner

Dell con0 now available

Press RETURN to get started.
13d21h10m: %RPM0-P:CP %SEC-5-LOGIN_SUCCESS: Login successful for user on
line console
This is the banner
Dell>
```

Related Commands [banner motd](#) — sets a Message of the Day banner.
[banner exec](#) — enables the display of a text string when you enter EXEC mode.



banner motd

Set a message of the day (MOTD) banner.

Syntax `banner motd c line c`
To delete a Message of the Day banner, enter **no banner motd**.

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, refer to the relevant *Dell 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.
9.0.2.0	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 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 banner EXEC (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.

Syntax

```
cam-acl {default | l2acl number ipv4acl number ipv6acl number ipv4qos  
number l2qos number l2pt number ipmacacl number [vman-qos | vman-dual-qos]  
number ecfmacacl number
```

Parameters

default

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

- L3 ACL (ipv4acl): 4
- L2 ACL(l2acl): 6
- IPv6 L3 ACL (ipv6acl): 0
- L3 QoS (ipv4qos): 2
- L2 QoS (l2qos): 1
- OpenFlow: 0 (disabled)
- FCoE (fcoeacl): 0 (disabled)
- iSCSI Optimization (iscsiptacl): 0 (disabled)

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 ipv6acl range must be a factor of 2.

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)

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.
9.0.2.0	Introduced on the S6000.
9.2(0.2)	Added support for the <code>fcoe</code> 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 <code>fcoeacl</code> and <code>iscsiptacl</code> on the S4810.
8.3.11.1	Introduced on the Z9000.



Version	Description
8.3.1.0	Added the keywords <code>ecfmac1</code> , <code>vman-qos</code> , and <code>vman-dual-qos</code> .
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 three blocks and these blocks cannot be reallocated. The `ipv4acl` profile range is from 1 to 4.

When configuring space for IPv6 ACLs, 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 you enabled BMP, 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.

clear line

Reset a terminal line.

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

Parameters

<i>line-number</i>	Enter a number for one of the 12 terminal lines on the system. The range is from 0 to 11.
aux 0	Enter the keywords <code>aux 0</code> to reset the auxiliary port.
console 0	Enter the keywords <code>console 0</code> to reset the console port.
<i>vty number</i>	Enter the keyword <code>vty</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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.
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.

Syntax `configure [terminal]`

Parameters

terminal	(OPTIONAL) Enter the keyword <code>terminal</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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.

Example

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

disable

Return to EXEC mode.

Syntax `disable [level]`



Parameters	<i>level</i>	(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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	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.
	9.0.2.0	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.
	7.6.1.0	Introduced on the S-Series.
	7.5.1.0	Introduced on the C-Series.
	E-Series	Original command.

do

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

Syntax	do <i>command</i>							
Parameters	<i>command</i>	Enter an EXEC-level command.						
Defaults	none							
Command Modes	· CONFIGURATION · INTERFACE							
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr></table>		Version	Description	9.7(0.0)	Introduced on the S6000-ON.	9.0.2.0	Introduced on the S6000.
Version	Description							
9.7(0.0)	Introduced on the S6000-ON.							
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.
7.6.1.0	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-5/1/1)#do clear counters
Clear counters on all interfaces [confirm]
Dell(conf-if-te-5/1/1)#
Dell(conf-if-te-5/1/1)#do clear logging
Clear logging buffer [confirm]
Dell(conf-if-te-5/1/1)#
Dell(conf-if-te-5/1/1)#do reload
System configuration has been modified. Save? [yes/no]: n
Proceed with reload [confirm yes/no]: n
```

enable

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

Syntax `enable [level]`

Parameters

<i>level</i>	(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, refer to the relevant *Dell 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(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, and MXL.
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.
8.3.12.0	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**.



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 optic-info-update interval

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

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
9.0.2.0	Introduced on the S6000.
8.3.19.0	Replacement command for the S4820T. Replaces the <code>enable xfp-power-updates</code> command.
8.3.11.4	Replacement command for the Z9000. Replaces the <code>enable xfp-power-updates</code> command



Version	Description
8.3.10.0	Replacement command for the S4810 only. Replaces the <code>enable xfp-power-updates</code> 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).

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, refer to the relevant *Dell 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.
9.0.2.0	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 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.

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, refer to the relevant *Dell 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.
9.0.2.0	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.
7.6.1.0	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 con0 is now available
Press RETURN to get started.
Dell>

exit

Return to the lower command mode.

Syntax `exit`



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, refer to the relevant *Dell 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.
9.0.2.0	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.

Related Commands [end](#) — returns to EXEC Privilege mode.

ftp-server enable

Enable FTP server functions on the system.

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
9.7(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.
8.3.11.1	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 Dell (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 tgting
 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>
```

ftp-server topdir

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

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
9.7(0.0)	Introduced on the S6000-ON.
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 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 Dell Networking OS directs users to the flash directory when logging in to the FTP server.

Related Commands [ftp-server enable](#) — enables FTP server functions on the E-Series.

[ftp-server username](#) — sets a username and password for incoming FTP connections to the E-Series.

ftp-server username

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

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

<i>username</i>	Enter a text string up to 40 characters long as the user name.
<i>password password</i>	Enter the keyword <code>password</code> then a string up to 40 characters long as the password. Without specifying an encryption type, the password is unencrypted.
<i>encryption-type</i>	(OPTIONAL) After the keyword <code>password</code> , enter one of the following numbers: • 0 (zero) for an unencrypted (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
9.7(0.0)	Introduced on the S6000-ON.
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 ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command.

hostname

Set the host name of the system.

Syntax `hostname name`

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

Defaults **Dell**

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.
9.0.2.0	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.



Version	Description
E-Series	Original command.

Usage Information The hostname is used in the prompt.

ip ftp password

Specify a password for outgoing FTP connections.

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

<i>encryption-type</i>	(OPTIONAL) Enter one of the following numbers: • 0 (zero) for an unencrypted (clear text) password • 7 (seven) for a hidden text password
<i>password</i>	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
9.7(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.
8.3.11.1	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

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

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[/subport] or number 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. The range is from 1 to 128.
- 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 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 8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
Version 8.2.1.0	Increased number of VLANs on ExaScale to 4094 (was 2094).
Version 8.1.1.0	Introduced on the E-Series ExaScale.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
E-Series	Original command.



ip tftp vrf

Configures an TFTP client with a VRF that is used to connect to the TFTP server.

Syntax	<pre>ip tftp [vrf vrf-name]</pre> To undo the TFTP client configuration, use the <code>no ip tftp [vrf vrf-name]</code> command.									
Parameters	vrf vrf-name	Enter the keyword <code>vrf</code> and then the name of the VRF to specify the VRF that is used by the TFTP client.								
Defaults	Disabled									
Command Modes	CONFIGURATION									
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.5(0.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.4.(0.0)</td><td>Introduced on the S-Series and Z9000.</td></tr></table>		Version	Description	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.
Version	Description									
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 make the TFTP clients VRF aware. The VRF name that you specify is used by the TFTP client to reach the TFTP server. If no VRF is specified, then the default VRF is used.									
Related Commands	ftp-server topdir — sets the directory to be used for incoming FTP connections. ftp-server username — sets a username and password for incoming FTP connections.									

ip ftp username

Assign a user name for outgoing FTP connection requests.

Syntax	<pre>ip ftp username username</pre> To return to anonymous FTP connections, use the <code>no ip ftp username [username]</code> 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.	



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.
9.0.2.0	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 Configure a password with the `ip ftp password` command.

Related Commands [ip ftp password](#) — sets the password for FTP connections.

ip ftp vrf

Configures an FTP client with a VRF that is used to connect to the FTP server.

Syntax `ip ftp [vrf vrf-name]`
To undo the FTP client configuration, use the `ip ftp [vrf vrf-name]` command.

Parameters

vrf vrf-name	Enter the keyword <code>vrf</code> and then the name of the VRF to specify the VRF that is used by the FTP client.

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
9.7(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 make the FTP clients VRF-aware. The VRF name that you specify is used by the FTP client to reach the FTP server. If no VRF name is specified, then the default VRF is used.



ip telnet server enable

Enable the Telnet server on the switch.

Syntax	<code>ip telnet server enable</code> To disable the Telnet server, use the <code>no ip telnet server enable</code> command.
Defaults	Enabled
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
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 server vrf

Configures the TELNET server on either a specific VRF or a management VRF.

Syntax	<code>ip telnet server vrf {management vrf-name}</code> To undo the TELNET server configuration, use the <code>no ip telnet server [vrf vrf-name]</code> command.				
Parameters	<table><tr><td>vrf management</td><td>Enter the keyword <code>vrf</code> followed by the keyword <code>management</code> to specify a management VRF that is used by the TELNET server.</td></tr><tr><td>vrf vrf-name</td><td>Enter the keyword <code>vrf</code> and then the name of the VRF to specify the VRF that is used by the TELNET server.</td></tr></table>	vrf management	Enter the keyword <code>vrf</code> followed by the keyword <code>management</code> to specify a management VRF that is used by the TELNET server.	vrf vrf-name	Enter the keyword <code>vrf</code> and then the name of the VRF to specify the VRF that is used by the TELNET server.
vrf management	Enter the keyword <code>vrf</code> followed by the keyword <code>management</code> to specify a management VRF that is used by the TELNET server.				
vrf vrf-name	Enter the keyword <code>vrf</code> and then the name of the VRF to specify the VRF that is used by the TELNET server.				
Defaults	Disabled				
Command Modes	CONFIGURATION				



Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.5(0.0)</td><td>Introduced on the Z9500.</td></tr> <tr> <td>9.4(0.0)</td><td>Introduced on the S-Series and Z9000.</td></tr> </table>	Version	Description	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.
Version	Description								
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	You can enable the TELNET server on either a management VRF or a user-defined VRF but not both. If you do not specify a VRF name, then the TELNET server is enabled on the default VRF.								
Example	<pre>Dell(config)#ip telnet server vrf vrf1 Dell(config)#no ip telnet server vrf Dell(config)#ip telnet server vrf management Dell(config)#no ip telnet server vrf</pre>								

ip telnet source-interface

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

Syntax	<pre>ip telnet source-interface <i>interface</i></pre> To return to the default setting, use the <code>no ip telnet source-interface [<i>interface</i>]</code> command.
Parameters	<i>interface</i> Enter the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For Loopback interfaces, enter the keyword <code>loopback</code> then a number from zero (0) to 16383. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094. - For a tunnel interface, enter the keyword <code>tunnel</code>.
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 <i>Dell Networking OS Command Line Reference Guide</i>. 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.
9.0.2.0	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.
8.2.1.0	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](#) — telnet to another device.

ip tftp vrf

Configures an TFTP client with a VRF that is used to connect to the TFTP server.

Syntax `ip tftp [vrf vrf-name]`
 To undo the TFTP client configuration, use the `no ip tftp [vrf vrf-name]` command.

Parameters

vrf vrf-name	Enter the keyword <code>vrf</code> and then the name of the VRF to specify the VRF that is used by the TFTP client.

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
9.7(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 make the TFTP clients VRF aware. The VRF name that you specify is used by the TFTP client to reach the TFTP server. If no VRF is specified, then the default VRF is used.

Related Commands [ftp-server topdir](#) — sets the directory to be used for incoming FTP connections.

[ftp-server username](#) — sets a username and password for incoming FTP connections.

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.

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

Parameters	aux 0	Enter the keyword aux 0 to configure the auxiliary terminal connection.
	console 0	Enter the keyword <code>console 0</code> to configure the console port. The console option for the S-Series is <0-0>.
	vtty number	Enter the keyword <code>vtty</code> then a number from 0 to 9 to configure a virtual terminal line for remote sessions. The system supports 10 remote 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
9.7(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.
8.3.11.1	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.



login concurrent-session

Configures the limit of concurrent sessions for all users 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 <i>number-of-sessions</i>	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, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

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

Version	Description
9.8(0.0)	Introduced on the S4810, S4820, S4048-ON, S3048-ON, 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:

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

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

```
Dell(conf)#login concurrent-session clear-line enable
Dell(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 user login statistics. By default, the system displays the login statistics for the last 30 days.
time-period <i>days</i>	Sets the number of days for which the system stores the user login statistics. The 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, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

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



Version	Description
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 and the details of any failed login attempts by others.

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 is not applicable for login sessions that do not use user names for authentication. 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: Mon Feb 16 04:36:11 2015 Line vty0 ( 10.14.1.97 ).
There were 2 unsuccessful login attempt(s) since the last successful login.
There were 3 unsuccessful login attempt(s) for user admin in last 30
day(s).
```

The preceding message shows that the user had previously logged in to the system using the VTY line from 10.14.1.97. 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: Wed Feb 5 14:05:28 IST 2015 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).
```

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 all users 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.

motd-banner

Enable a message of the day (MOTD) banner to appear when you log in to the system.

Syntax `motd-banner`

To disable the MOTD banner, use the `no motd-banner` command.

Defaults Enabled on all 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
9.7(0.0)	Introduced on the S6000-ON.
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 ExaScale
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

ping

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

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 format, to which you are testing connectivity.



NOTE: The `::` notation specifies successive hexadecimal fields of zeros.



<i>count</i>	Enter the number of echo packets to be sent. The default is 5. • number: from 1 to 2147483647 • continuous: transmit echo request continuously
<i>datagram size</i>	Enter the ICMP datagram size. The range is from 36 to 15360 bytes. The default is 100.
<i>timeout</i>	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.
<i>source</i>	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 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094. • For a Tunnel interface, enter the keyword <code>tunnel</code> then a number from 1 to 16383.
<i>tos</i>	(IPv4 only) Enter the type of service required. The range is from 0 to 255. The default is 0.
<i>df-bit</i>	(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.
<i>validate-reply</i>	(IPv4 only) Enter Y or N for reply validation. • N: Do not validate reply data. • Y: Do validate reply data. Default is No.
<i>outgoing-interface</i>	(IPv6 link-local address) Enter the outgoing interface for ping packets to a destination link-local address.
<i>pattern pattern</i>	(IPv4 only) Enter the IPv4 data pattern. Range: 0-FFFF. Default: 0xABCD.
<i>sweep-min-size</i>	Enter the minimum size of datagram in sweep range. The range is from 52 to 15359 bytes.
<i>sweep-max-size</i>	Enter the maximum size of datagram in sweep range. The range is from 53 to 15359 bytes.
<i>sweep-interval</i>	Enter the incremental value for sweep size. The range is from 1 to 15308 seconds.
<i>interface</i>	(IPv4 only) Enter the outgoing interface for multicast packets. Enter the IP address in A.B.C.D format. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> 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.

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 9.0.2.0	Introduced on the S6000.
Version 9.0.0.0	Introduced on the Z9000.
Version 8.3.19.0	Introduced on the S4820T.
	Added support for the <code>outgoing-interface</code> option for link-local IPv6 addressing on the S4820T.
Version 8.3.12.0	Added support for the <code>outgoing-interface</code> option for link-local IPv6 addressing on the S4810.
Version 8.3.11.1	Introduced on the Z9000.
Version 8.3.7.0	Introduced on the S4810.
Version 8.5.1.0	Added support for 4-port 40G line cards on the ExaScale.
Version 8.4.1.0	IPv6 ping is available on management interface.
Version 8.3.1.0	Introduced extended ping options.
Version 8.2.1.0	Introduced on the E-Series ExaScale (IPv6).
Version 8.1.1.0	Introduced on the E-Series ExaScale (IPv4).
Version 7.9.1.0	Introduced VRF.
Version 7.6.1.0	Introduced on the S-Series.
Version 7.5.1.0	Introduced on the C-Series.
Version 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.

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.



Symbol	Description
.	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.
&	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#
```

reload

Reboot Dell Networking Operating System (OS).

Syntax	<code>reload [conditional <i>nvr</i>am-<i>c</i>fg-<i>c</i>hange]</code>	
Parameters	conditional <i>nvr</i>am-<i>c</i>fg-<i>c</i>hange	Reload if the condition is true. A configuration change to the nvram requires a switch reload. To reload the switch, select <i>nvr</i> am- <i>c</i> fg- <i>c</i> hange.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	Introduced on the S6000.



Version	Description
9.0.0.0	Introduced on the Z9000.
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, FTOS 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.

send

Send messages to one or all terminal line users.

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
9.7(0.0)	Introduced on the S6000-ON.
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 ExaScale.
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 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.

Syntax `service timestamps [debug | log] [datetime [localtime] [msec] [show-timezone] | uptime]`

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

Parameters

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

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.
9.0.2.0	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.



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.

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

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

show alarms

View alarms currently active in the system.

Syntax `show alarms [threshold]`

Parameters

threshold (OPTIONAL) Enter the keyword `threshold` to display the temperature thresholds in Celcuis for each level.

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
9.7(0.0)	Introduced on the S6000-ON.
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 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 alarms
-- Minor Alarms --
Alarm Type Duration
```



```

-----
RPM 0 PEM A failed or rmvd 7 hr, 37 min
SFM 0 PEM A failed or rmvd 7 hr, 37 min
SFM 1 PEM A failed or rmvd 7 hr, 37 min
SFM 2 PEM A failed or rmvd 7 hr, 37 min
SFM 3 PEM A failed or rmvd 7 hr, 37 min
SFM 4 PEM A failed or rmvd 7 hr, 37 min
SFM 5 PEM A failed or rmvd 7 hr, 37 min
SFM 6 PEM A failed or rmvd 7 hr, 37 min
SFM 7 PEM A failed or rmvd 7 hr, 36 min
stack-unit 1 PEM A failed or rmvd 7 hr, 36 min
stack-unit 4 PEM A failed or rmvd 7 hr, 36 min
only 8 SFMs in chassis 7 hr, 35 min

-- Major Alarms --

Alarm Type Duration
-----
No major alarms
Dell#

```

show command-tree

Display the entire CLI command tree, and optionally, display the utilization count for each command and its options.

Syntax `show command-tree [count | no]`

Parameters

count	Display the command tree with a usage counter for each command.
no	Display all of the commands that may be preceded by the keyword <code>no</code> , which is the keyword used to remove a command from the running-configuration.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.2.1.0	Introduced.

Usage Information Reload the system to reset the command-tree counters.



Example

```
Dell#show command-tree count
!
Enable privilege mode:

enable command usage:3
  <0-15> option usage: 0

exit    command usage:1

show    command-tree command usage:9
count option usage: 3

show version command usage:1
!
Global configuration mode:

aaa authentication enable command usage:1
  WORD    option usage: 1
  default option usage: 0
  enable  option usage: 0
  line    option usage: 0
  none    option usage: 0
  radius  option usage: 1
  tacacs+ option usage: 0
```

show cpu-traffic-stats

View the CPU traffic statistics.

Syntax

```
show cpu-traffic-stats [port number | all | cp ]
```

Parameters

<i>port number</i>	(OPTIONAL) Enter the port number to display traffic statistics on that port only. The range is from 1 to 1568.
<i>all</i>	(OPTIONAL) Enter the keyword <i>all</i> to display traffic statistics on all the interfaces receiving traffic, sorted based on the traffic.
<i>cp</i>	(OPTIONAL) Enter the keyword <i>cp</i> to display traffic statistics on the specified CPU.

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
9.7(0.0)	Introduced on the S6000-ON.
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.



Version	Description
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 TenGigabitEthernet 8/2/1 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 8/2/1 Total packets:500
LLC:0, SNAP:0, IP:500, ARP:0, other:0
Unicast:500, Multicast:0, Broadcast:0
Received 37% traffic on TenGigabitEthernet 8/1/1 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#
```

show debugging

View a list of all enabled debugging processes.

Syntax `show 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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
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.

Example

show environment

View S-Series and Z-Series system component status (for example, temperature or voltage).

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

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

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
9.7(0.0)	Introduced on the S6000-ON.
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 <code>show environment fan</code> 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)

```
Dell#show environment
```

```
-- Fan Status --
Unit Bay TrayStatus Fan0 Speed Fan1 Speed
-----
0 0 up up 6971 up 7072
0 1 up up 6971 up 7021
0 2 up up 7021 up 7021
```

Speed in RPM

```
-- Power Supplies --
Unit Bay Status Type FanStatus FanSpeed(rpm)
-----
0 0 down UNKNOWN down 0
0 1 up AC up 6504
```

```
-- Unit Environment Status --
Unit Status Temp Voltage TempStatus
-----
* 0 online 36C ok 1
```

* Management Unit

```
-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1 Sensor2 Sensor3 Sensor4 Sensor5 Sensor6
-----
0 40 36 37 37 31 31 46
```

```
Dell#show environment fan
```

```
-- Fan Status --
Unit Bay TrayStatus Fan0 Speed Fan1 Speed
-----
0 0 up up 7021 up 7021
0 1 up up 6971 up 7072
0 2 up up 7021 up 6971
```

Speed in RPM

```
Dell#show environment pem
```

```
-- Power Supplies --
Unit Bay Status Type FanStatus FanSpeed(rpm)
-----
0 0 down UNKNOWN down 0
0 1 up AC up 6504
```

```
Dell#show environment thermal-sensor
```

```
-- Thermal Sensor Readings (deg C) --
Unit Sensor0 Sensor1 Sensor2 Sensor3 Sensor4 Sensor5 Sensor6
-----
0 39 36 37 37 31 31 46
```

show inventory

Display the S-Series or Z-Series switch type, components (including media), and Dell Networking Operating System (OS), including hardware identification numbers and configured protocols.

Syntax `show inventory [media slot]`



Parameters

media slot(OPTIONAL) Enter the keyword `media` then the stack ID of the stack member for which you want to display the media information.**NOTE:** This parameter is available but not supported in Dell Networking Operating System version 9.7(0.0) and earlier. If you use this parameter, the output displays “Media not present or accessible”.

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 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.
9.0.2.0	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.
8.3.11.4	Output expanded to include Piece Part ID (PPID) and eSR4 optics.
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

If there are no fiber ports in the unit, just the header under *show inventory media* displays. If there are fiber ports but no media is present or accessible.

Example (S6000)

Dell#show inventory

```

System Type       : S6000
System Mode       : 1.0
Software Version   : 9-4 (0-168)

```

Unit	Type	Serial Number	Part Number	Rev	Piece Part ID
* 0	S6000-01-FE-32T	NA	08YWFG	A00	CN-08YWFG-28298-39Q-0015 A00
0	S6000-PWR-AC	NA	0T9FNW	A00	CN-0T9FNW-28298-39Q-0005 A00
0	S6000-FAN	NA	0MGDH8	A00	CN-0MGDH8-28298-39Q-0009 A00
0	S6000-FAN	NA	0MGDH8	A00	CN-0MGDH8-28298-39Q-0007 A00
0	S6000-FAN	NA	0MGDH8	A00	CN-0MGDH8-28298-39Q-0008 A00

* - Management Unit

Software Protocol Configured

LLDP

Example

Dell#show inventory media

Slot	Port	Type	Media	Serial Number	F10Qualified
0	0	QSFP	40GBASE-CR4-1M	APF11200012UQQ	Yes
0	1	QSFP	40GBASE-CR4-1M	APF11200012UQQ	Yes
0	2	QSFP	40GBASE-CR4-1M	APF11200012UQQ	Yes
0	3	QSFP	40GBASE-CR4-1M	APF11200012UQQ	Yes
0	4	QSFP	40GBASE-CR4-1M	APF11200012UR1	Yes
0	5	QSFP	40GBASE-CR4-1M	APF11200012UR1	Yes
0	6	QSFP	40GBASE-CR4-1M	APF11200012UR1	Yes



0	7	QSFP	40GBASE-CR4-1M	APF11200012UR1	Yes
0	8	QSFP	40GBASE-CR4-1M	APF12300017GEY	Yes
0	9	QSFP	40GBASE-CR4-1M	APF12300017GEY	Yes
0	10	QSFP	40GBASE-CR4-1M	APF12300017GEY	Yes

Related Commands

- [show interfaces](#) — displays the interface configuration.

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

Parameters

all	(Optional)Displays the login statistics of all users 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 <code>unsuccessful-attempts</code> 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
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.
time-period days	(Optional)Displays the number of failed login attempts by the current user in the specified period.

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
9.8(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.

```
Dell#show login statistics
```

```
-----
User: admin
Last login time: Mon Feb 16 04:40:00 2015
Last login location: Line vty0 ( 10.14.1.97 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 30 day(s): 3
-----
```

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

```
Dell#show login statistics all
```

```
-----
User: admin
Last login time: Mon Feb 16 04:40:00 2015
Last login location: Line vty0 ( 10.14.1.97 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 7 day(s): 3
-----
```

```
-----
User: secadm
Last login time: Mon Feb 16 04:45:29 2015
Last login location: Line vty0 ( 10.14.1.97 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 7 day(s): 0
-----
```

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

```
Dell#show login statistics user admin
```

```
-----
User: admin
Last login time: Mon Feb 16 04:40:00 2015
Last login location: Line vty0 ( 10.14.1.97 )
Unsuccessful login attempt(s) since the last successful login: 0
Unsuccessful login attempt(s) in last 11 day(s): 3
-----
```

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

```
Dell#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.

```
Dell#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.

```
Dell#show login statistics unsuccessful-attempts user admin
There were 3 unsuccessful login attempt(s) for user admin in last 12
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 all users on console and virtual terminal lines.

show memory

View current memory usage on the switch.

Syntax `show memory [stack-unit id]`

Parameters

stack-unit id	(OPTIONAL) Enter the keyword <code>stack-unit</code> then the stack unit ID of the S-Series stack member to display memory information on the designated stack member. The unit ID range from 1 to 6.

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
97(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced this version of the command for the S-Series.

Usage Information The output for `show memory` displays the memory usage of LP part (sysdlp) of the system. The sysdlp is an aggregate task that handles all the tasks running on the S-Series' CPU.



Example

```
Dell#show memory stack-unit 1
Statistics On Unit 1 Processor
=====
Total(b)  Used(b)  Free(b)    Lowest(b)  Largest(b)
268435456 4010354 264425102 264375410 264425102
```

Example (S4820T)

```
Dell#show memory stack 0
Statistics On Unit 0 Processor
=====
Total(b)  Used(b)  Free(b)    Lowest(b)  Largest(b)
2147483648 4322398 2143161250 2142548382 2143161250
Dell#
```

show processes cpu

Display CPU usage information based on processes running.

Syntax

```
show processes cpu [management-unit 1-99 [details] | stack-unit id |
summary | [stack-unit id]]
```

Parameters

management-unit 1-99 [details]	(OPTIONAL) Display processes running in the control processor. The 1-99 variable sets the number of tasks to display in order of the highest CPU usage in the past five (5) seconds. Add the keyword <code>details</code> to display all running processes (except <code>sysdp</code>). Refer to Example (management-unit).
stack-unit id	(OPTIONAL) Enter the keyword <code>stack-unit</code> then the stack member ID. As an option of the <code>show processes cpu</code> command, this option displays CPU usage for the designated stack member. Or, as an option of the <code>command</code> , this option limits the output of memory statistics to the designated stack member. . Refer to Example (stack-unit).
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view CPU utilization of processes related to stack-unit processing.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.



Version	Description
8.3.7.0	Introduced on the S4810.
7.7.1.0	Added the keywords management-unit [details].
7.6.1.0	Introduced on the S-Series.

Example

```
Dell#show processes cpu ?
management-unit      Management Unit
stack-unit           Unit Number
summary              Summary of CPU utilization
|                   Pipe through a command
```

```
Dell#show processes cpu summary
```

```
CPU utilization      5Sec    1Min    5Min
-----
UNIT0                3%      3%      1%
Dell#show processes cpu stack-unit 0
```

```
CPUID      5sec      1min      5min
-----
CORE 0      13.17      11.53      0.00
CORE 2       9.38      12.16      0.00
Overall     11.28      11.84      0.00
```

```
CPU utilization of sysdpl for five seconds: 2%/0%; one minute: 3%; five
minutes: 1%
```

```
PID      Runtime(ms)   Invoked    uSecs    5Sec    1Min    5Min
TTY      Process
0xbb773000 5950      595        10000    1.00%   2.25%   1.22%
0         tExcTask
0xbab2a000 4030      403        10000    1.00%   1.33%   0.73%
0         frrpagt
0xbacf3000 10        1          10000    0.00%   0.00%   0.00%
0         F10StkMgr
0xbad0c000 710       71         10000    0.00%   0.00%   0.03%
0         lcMgr
0xbad24000 30        3          10000    0.00%   0.00%   0.00%
0         dla
0xbad44000 50        5          10000    0.00%   0.00%   0.00%
0         sysAdmTsk
0xbad58000 650       65         10000    0.00%   0.00%   0.00%
0         timerMgr
0xbad6e000 50        5          10000    0.00%   0.00%   0.00%
0         PM
0xbad85000 1190      119        10000    0.00%   0.00%   0.00%
0         KP
0xbad9a000 0         0          0        0.00%   0.00%   0.00%
0         evagt
0xbadb4000 30        3          10000    0.00%   0.00%   0.00%
0         ipc
0xbadc9000 10        1          10000    0.00%   0.00%   0.00%
0         sysReaper
0xbae22000 60        6          10000    0.00%   0.00%   0.02%
0         tme
```

```
Dell#show processes cpu management-unit ?
<1-99>          Number of tasks with highest CPU usage last 5
seconds
details         Detail CPU utilization
|              Pipe through a command
Dell#show processes cpu management-unit details
```

```
CPUID      5sec      1min      5min
-----
CORE 0      11.73      10.79      12.82
```



CORE 2	11.73	12.05	14.31
Overall	11.73	11.42	13.56

PID	Runtime (ms)	Invoked	uSecs	5Sec	1Min	5Min
TTY	Process					
Process: system	PID: 0	CPU usage: 5sec - 13.12%	1min - 13.37%			
5min - 12.94%	CoreID: 3					
Process: sysd	PID: 428	CPU usage: 5sec - 3.78%	1min - 2.56%			
5min - 3.40%	CoreID: 0					
Process: sysd	PID: 410	CPU usage: 5sec - 1.59%	1min - 0.96%			
5min - 2.50%	CoreID: 2					

5Min	TTY	TID	Runtime (ms)	Invoked	uSecs	5Sec	1Min
		Thread					
0.00%	0	56	20	2	10000	0.00%	0.00%
			usm				
0.00%	0	55	10	1	10000	0.00%	0.00%
			DHCLIENT				
0.00%	0	54	0	0	0	0.00%	0.00%
			cms				
0.00%	0	53	60	6	10000	0.00%	0.00%
			portmirr				
0.00%	0	52	0	0	0	0.00%	0.00%
			cfgDataSync				
0.00%	0	51	0	0	0	0.00%	0.00%
			sysCompMgr				
0.00%	0	50	50	5	10000	0.00%	0.01%
			statMgr				
0.08%	0	49	1010	101	10000	0.05%	0.07%
			sflCp				
0.00%	0	48	30	3	10000	0.00%	0.00%
			snmp				
0.00%	0	47	0	0	0	0.00%	0.00%
			dpi_cmow				
0.00%	0	46	0	0	0	0.00%	0.00%
			dpi_taskcmo				

```

Dell#show processes cpu management-unit details ?
| Pipe through a command
Dell#show processes cpu management-unit ?
<1-99> Number of tasks with highest CPU usage last 5
seconds
details Detail CPU utilization
| Pipe through a command

```

Dell#show processes cpu management-unit

CPUID	5sec	1min	5min
-----	-----	-----	-----
CORE 0	9.54	9.92	12.82
CORE 2	10.74	11.56	14.31
Overall	10.14	10.74	13.56

PID	Runtime (ms)	Invoked	uSecs	5Sec	1Min	5Min
TTY	Process					
0x00000000	45040	4504	10000	13.12%	13.20%	12.94%
0	system					
0x000001ac	25750	2575	10000	2.78%	2.48%	3.40%
0	sysd					
0x0000019a	10650	1065	10000	0.60%	1.16%	2.50%
0	sysd					
0x000003a5	860	86	10000	0.40%	0.22%	0.28%
0	clish					
0x000001ad	520	52	10000	0.20%	0.30%	0.16%
0	lacp					
0x000004ba	330	33	10000	0.20%	0.36%	0.09%
0	clish					
0x000000c9	1240	124	10000	0.20%	0.15%	0.44%
0	nvmgr					
0x000000e0	530	53	10000	0.20%	0.12%	0.16%
0	igmp					



0x00000132	420	42	10000	0.20%	0.10%	0.13%
0	vrrp					
0x0000028d	410	41	10000	0.20%	0.05%	0.12%
0	ovsdbsvr					
0x000000a9	200	20	10000	0.20%	0.03%	0.06%
0	arpd					
0x00000253	100	10	10000	0.20%	0.02%	0.02%
0	otm					
0x00000206	140	14	10000	0.20%	0.02%	0.03%
0	tnlmgr					
0x00000012	1290	129	10000	0.00%	0.10%	0.12%
0	mount_mfs					
0x0000024d	400	40	10000	0.00%	0.08%	0.14%
0	xstp					

Related Commands [show hardware layer2 acl](#) — displays Layer 2 ACL data for the selected stack member and stack member port-pipe.

[show hardware layer3](#) — displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

[show hardware stack-unit](#) — displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

[show hardware system-flow](#) — displays Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

[show interfaces stack-unit](#) — displays information on all interfaces on a specific S-Series stack member.

[show processes memory \(S-Series\)](#) — displays CPU usage information based on processes running in an S-Series.

show processes ipc flow-control

Display the single window protocol queue (SWPQ) statistics.

Syntax `show processes ipc flow-control [cp | rp1 | rp2 | stack-unit]`

Parameters

cp	(OPTIONAL) Enter the keyword <code>cp</code> to view the control processor's SWPQ 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
9.7(0.0)	Introduced on the S6000-ON.

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.
8.3.12.0	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
#of to / Timeout	Timeout count
#of Retr /Retries	Number of retransmissions
#msg Sent/Msg Sent/	Number of messages sent
#msg Ackd/Ack Rcvd	Number of messages acknowledged
Retr /Available Retra	Number of retries left
Total/ 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.
- In the S-Series example, a retry (Retries) value of zero indicates that the SWP mechanism reached the maximum number of retransmissions without an acknowledgement.

Example (S-Series)

```
Dell#show processes ipc flow-control ?
cp          Control Processor
|           Pipe through a command
```



show processes memory

Display memory usage information based on processes running in the S-Series or Z-Series system.

Syntax `show processes memory {management-unit | stack unit {unit-id | all | summary}}`

Parameters	management-unit	Enter the keyword <code>management-unit</code> for CPU memory usage of the stack management unit.
	stack unit unit id	Enter the keyword <code>stack unit</code> then a stack unit ID of the member unit for which to display memory usage on the forwarding processor.
	all	Enter the keyword <code>all</code> for detailed memory usage on all stack members.
	summary	Enter the keyword <code>summary</code> for a brief summary of memory availability and usage on all stack members.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
7.7.1.0	Added the <code>management-unit</code> option.
7.6.1.0	Introduced on the S-Series.

Usage Information	show processes memory output Field	Description
	Total:	Total system memory available
	MaxUsed:	Total maximum memory used ever (history indicated with 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



show processes	Description
memory output	
Field	
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 the `show process memory` command displays the memory usage statistics running on CP part (sysd) of the system. The sysd is an aggregate task that handles all the tasks running on S-Series' CP.

For the S-Series, the output of the `show memory` command and this command differ based on which FTOS processes are counted.

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

Example

```
Dell#show processes memory stack-unit 1
Total: 268435456, MaxUsed: 2420244, CurrentUsed: 2420244, CurrentFree:
266015212
TaskName TotalAllocated TotalFreed MaxHeld CurrentHolding
tme      435406          397536    54434    37870
ipc      16652           0      16652    16652
timerMgr 33304              0      33304    33304
sysAdmTsk 33216            0      33216    33216
tFib4    1943960          0    1943960  1943960
aclAgent 90770            16564    74206    74206
ifagt_1  21318            16564    21318    4754
dsagt_   6504             0       6504    6504
MacAgent 269778            0     269778  269778
```

Example (management-unit)

```
Dell#show processes management-unit

Total      : 151937024,   MaxUsed : 111800320 [2/25/2008 4:18:53]
CurrentUsed: 98848768, CurrentFree: 53088256

SharedUsed : 13007848, SharedFree : 7963696
PID Process      ResSize      Size Allocs Frees      Max Current
337 KernLrnAgMv 117927936      0      0      0      0      0
331 vrrp         5189632    249856    50572      0    50572    50572
323 frrp         5206016    241664   369238      0   369238   369238
322 xstp         7430144   2928640   38328      0    38328   38328
321 pim          5267456    823296    62168      0    62168   62168
314 igmp         4960256    380928   18588   16564   18588    2024
313 mrtm         6742016   1130496    72758      0    72758   72758
308 l2mgr        5607424    552960   735214   380972   619266   354242
301 l2pm         5001216    167936  1429522  1176044   286606   253478
298 arpm         4628480    217088    71092   33128    71092   37964
294 ospf         5468160    503808   724204   662560    78208   61644
288 dsm          6778880   1159168   39490   16564   39490   22926
287 rtm          5713920    602112   442280   198768   376024   243512
284 rip          4562944    258048     528      0     528     528
281 lacp          4673536    266240   221060      0   221060   221060
277 ipml         4837376    380928   83788      0    83788   83788
```



```

273 acl          5005312  512000 239564 149076 123616 90488
272 topoDPC     117927936 0        0        0        0        0
271 bcmNHOP     117927936 0        0        0        0        0
270 bcmDISC     117927936 0        0        0        0        0
269 bcmATP-RX   117927936 0        0        0        0        0
268 bcmATP-TX   117927936 0        0        0        0        0
267 bcmSTACK    117927936 0        0        0        0        0
266 bcmRX       117927936 0        0        0        0        0
265 bcmLINK.0   117927936 0        0        0        0        0
!----- output truncated -----!

```

show software ifm

Display interface management (IFM) data.

Syntax `show software ifm {clients [summary] | ifagt number | ifcb interface | stack-unit unit-ID | trace-flags}`

Parameters

clients	Enter the keyword <code>clients</code> to display IFM client information.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to display brief information about IFM clients.
ifagt <i>number</i>	Enter the keyword <code>ifagt</code> then the number of an interface agent to display software pipe and IPC statistics.
ifcb <i>interface</i>	Enter the keyword <code>ifcb</code> then one of the following interface IDs then the slot/port[/subport] information to display interface control block information for that interface: - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
stack-unit <i>unit-ID</i>	Enter the keyword <code>stack-unit</code> then the stack member number to display IFM information for that unit.  NOTE: This option is only available on the S-Series.
trace-flags	Enter the keyword <code>trace-flags</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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.
8.5.1.0	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 0x0006e002 0x00000000 0x00000000 0x00000000 0
Dell#
```

show system

Display the status of all stack members or a specific member.

Syntax `show system [brief | stack-unit unit-id [disabled-ports] | stack-ports {status | topology}]`

Parameters

brief	(OPTIONAL) Enter the keyword <code>brief</code> to view an abbreviated list of system information.
stack-unit <i>unit-id</i>	(OPTIONAL) Enter the keywords <code>stack-unit</code> then the stack member ID for information on that stack member.
stack-ports <i>status</i> <i>topology</i>	(OPTIONAL) Enter the keywords <code>stack-ports</code> 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, refer to the relevant *Dell 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.
9.4(0.0)	Added support for the <code>disabled-ports</code> parameter .
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.
8.3.11.4	The <code>brief</code> parameter no longer displays the current Reload mode. To display Reload mode, use the <code>show reload-type</code> command. Modified the <code>show system stack-unit</code> 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 (show system stack unit – disabled ports)

```
Dell#show system stack-unit 1 disabled-ports
Disabled ports in stack-unit 1
      Disabled
          52
          56
          60
```

Example (show system brief)

```
Dell#sh system brief

Stack MAC           : 00:00:00:00:00:00
Reload-Type         : normal-reload [Next boot : normal-reload]

-- Stack Info --
Unit  UnitType      Status      ReqTyp      CurTyp      Version      Ports
-----
  1  Management  Software Failure  S6000-ON    S6000-ON    9-7 (0-288)  128
  2  Member      not present
  3  Member      not present
  4  Member      not present
  5  Member      not present
  6  Member      not present

-- Power Supplies --
Unit  Bay  Status      Type  FanStatus  FanSpeed (rpm)
-----
  1    1    up          AC    up         18528
  1    2    absent      AC    absent     0

-- Fan Status --
Unit  Bay  TrayStatus  Fan0  Speed  Fan1  Speed
-----
  1    1    up          up    19660  up    19275
  1    2    absent
  1    3    up          up    19275  up    18904
```



Speed in RPM

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

Related Commands

- [show version](#) – displays the Dell Networking OS version.
- [show hardware stack-unit](#) – displays the data plane and management plane input and output statistics of a particular stack member.

show tech-support

Display a collection of data from other `show` commands, necessary for Dell Networking technical support to perform troubleshooting.

Syntax `show tech-support [stack-unit unit-id | page]`

Parameters

stack-unit	(OPTIONAL) Enter the keywords <code>stack-unit</code> to view CPU memory usage for the stack member designated by <code>unit-id</code> .
page	(OPTIONAL) Enter the keyword <code>page</code> 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. When using the pipe command (<code> </code>), enter one of these keywords to filter command output. For details about filtering commands, refer to CLI Basics .
save	Enter the keyword <code>save</code> to save the command output. <code>flash:</code> Save to local flash drive (<code>flash://filename</code>). A maximum of 20 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 version history for this command.



Version	Description
97(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 save to the file options.
7.6.1.0	Introduced on the S-Series.

Usage Information

Without the `page` or `stack-unit` 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 version`
- `show clock`
- `show running-config`
- `show system stack-ports`
- `show interfaces`
- `show process memory`
- `show process cpu`
- `show file system`
- `show system`
- `show environment`
- `show ip traffic`
- `show ip management route`
- `show ip route summary`
- `show Inventory`
- `show log summary`
- `show command-history (last 20 commands)`
- `show log`

Example (S-Series)

```
Dell#show tech-support ?
page          Page through output
stack-unit    Unit Number
|            Pipe through a command
<cr>
Dell#show tech-support stack-unit 1 ?
|            Pipe through a command
<cr>
Dell#show tech-support stack-unit 1 | ?
except        Show only text that does not match a pattern
find          Search for the first occurrence of a pattern
grep          Show only text that matches a pattern
```



```

no-more      Don't paginate output
save         Save output to a file

Dell#show tech-support stack-unit 1 | save ?
flash:       Save to local file system (flash://filename (max 20
chars) )

Dell#show tech-support stack-unit 1 | save flash://LauraSave
Start saving show command report .....
Dell#

Dell#dir
Directory of flash:
1  drw-  16384   Jan 01 1980 00:00:00 +00:00 .
2  drwx  1536    Jul 13 1996 02:38:06 +00:00 ..
3  d---  512     Nov 20 2007 15:46:44 +00:00 ADMIN_DIR

```

Example (S-Series)

```

Dell#show tech-support stack-unit 0

----- show version
-----
Dell Real Time Operating System Software
Dell Operating System Version: 2.0
Dell Application Software Version: 9-4(0-168)
Copyright (c) 1999-2014 by Dell Inc. All Rights Reserved.
Build Time: Sun Mar 23 22:17:49 PDT 2014
Build Path: /work.local/build/buildSpaces/build01/E9-4-0/SW/SRC
Dell Networking OS uptime is 32 minute(s)

System image file is "s6000"

System Type: S6000
Control Processor: Intel Centerton with 3203911680 bytes of memory,
core(s) 2.

16G bytes of boot flash memory.

1 32-port TE/FG (SI)
64 Ten GigabitEthernet/IEEE 802.3 interface(s)
16 Forty GigabitEthernet/IEEE 802.3 interface(s)

----- show clock
-----
18:10:52.864 UTC Tue Mar 25 2014

----- show running-config
-----
Current Configuration ...
! Version 9-4(0-168)
! Last configuration change at Tue Mar 25 17:43:06 2014 by admin
!
boot system stack-unit 0 primary tftp://10.16.127.146/s6000
boot system stack-unit 0 secondary system: B:
boot system stack-unit 0 default system: A:
!
redundancy auto-synchronize full
redundancy disable-auto-reboot stack-unit
!
redundancy disable-auto-reboot stack-unit 0
redundancy disable-auto-reboot stack-unit 1
redundancy disable-auto-reboot stack-unit 2
redundancy disable-auto-reboot stack-unit 3
redundancy disable-auto-reboot stack-unit 4
redundancy disable-auto-reboot stack-unit 5
!
hardware watchdog stack-unit 0
hardware watchdog stack-unit 1
hardware watchdog stack-unit 2

```



```
hardware watchdog stack-unit 3
hardware watchdog stack-unit 4
hardware watchdog stack-unit 5
!
```

Related Commands

ssh-peer-stack-unit

Open an SSH connection to the peer stack-unit.

Syntax `ssh-peer-stack-unit [-l username]`

Parameters

`-l username` (OPTIONAL) Enter the keyword `-l` then your user name. The default is the user name associated with the terminal.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.3.11.1	Introduced on the S-Series.

telnet

Connect through Telnet to a server. The Telnet client and server in Dell Networking support IPv4 and IPv6 connections. You can establish a Telnet session directly to the router or a connection can be initiated from the router.

 **NOTE: The Telnet server and client are VRF-aware. Using the `vrf` parameter in this command, you can make a Telnet server or client to listen to a specific VRF. This capability enables a Telnet server or client to look up the correct routing table and establish a connection.**

Syntax `telnet {host | ip-address | ipv6-address prefix-length | vrf vrf instance name } [/source-interface]`

Parameters

`host` Enter the name of a server.

<i>ip-address</i>	Enter the IPv4 address in dotted decimal format of the server.
<i>ipv6-address prefix-length</i>	Enter the IPv6 address in the 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.	
<i>vrf instance</i>	(Optional) Enter the keyword <code>vrf</code> then the VRF instance name.
<i>source-interface</i>	(OPTIONAL) Enter the keywords <code>/source-interface</code> then the interface information to include the source interface. Enter the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a Null interface, enter the keyword <code>null</code> then the Null interface number. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For Tunnel interface types, enter the keyword <code>tunnel</code> then the slot/ port information. The range is from 1 to 16383. - For a VLAN interface, enter the keyword <code>vlan</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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. Added support for <i>source-interface</i> 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).
7.6.1.0	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.

Usage Information

The VRF configured using this command has a higher precedence than a VRF configured using the `ip telnet vrf vrf-name` command. If you do not use the VRF attribute in this command, then TELNET client uses the VRF configured using the `ip telnet vrf vrf-name` command.

The source interface configured using this command has a higher precedence than the source interface configured using the `ip telnet source-interface` command. If you do not configure a source interface using this command, then the TELNET client uses the source interface configured using the `ip telnet source-interface` command.

In case there is a mismatch between the VRF telnet source interface and the telnet VRF, then an error is reported.

Example

```
Dell#telnet vrf vrf1 10.10.10.2
```

telnet-peer-stack-unit

Open a Telnet connection to the peer stack unit.

Syntax `telnet-peer-stack-unit`

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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.3.11.1	Introduced on the S-Series.



terminal length

Configure the number of lines displayed on the terminal screen.

Syntax `terminal length screen-length`

Parameters

<i>screen-length</i>	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
9.7(0.0)	Introduced on the S6000-ON.
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 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.

Syntax `traceroute {host | ip-address | ipv6-address}`

Parameters

<i>host</i>	Enter the name of device.
<i>ip-address</i>	Enter the IP address of the device in dotted decimal format.
<i>ipv6-address</i>	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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.2.1.0	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.
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.Dell Networking.com

Translating "www.Dell Networking.com"...domain server (10.11.0.1) [OK]
Type Ctrl-C to abort.
```

```
-----
Tracing the route to www.Dell Networking.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.Dell Networking.com (10.11.30.126) 005.000 ms 001.000
ms 001.000 ms
3    fw-sjc-01.Dell Networking.com (10.11.127.254) 000.000 ms 000.000 ms
000.000 ms
4    www.Dell Networking.com (10.11.84.18) 000.000 ms 000.000 ms 000.000 ms
FTOS#

```

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

FTOS#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.

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
9.7(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.
8.3.11.1	Introduced on the Z9000.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.



Version	Description
7.5.1.0	Introduced on the C-Series.
E-Series	Original command

virtual-ip

Configure a virtual IP address for the active management interface. You can configure virtual addresses both for IPv4 and IPv6 independently.

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
9.7(0.0)	Introduced on the S6000-ON.
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.

Syntax `write {memory compressed| terminal}`

Parameters	memory	Enter the keyword <code>memory</code> to copy the current running configuration to the startup configuration file. This command is similar to the <code>copy running-config startup-config</code> command.
	compressed	Enter the keyword <code>compressed</code> to write the operating configuration to the startup-config file in the compressed mode.
	terminal	Enter the keyword <code>terminal</code> to copy the current running configuration to the terminal. This command is similar to the <code>show running-config</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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 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" (for example, you used a specific file during the `boot config` command), the running-config is not saved to that file; use the `copy` command to save any running-configuration changes to that local file.



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 operating software supports remote authentication dial-in service (RADIUS) and active directory environments using 802.1X Port Authentication.

Important Points to Remember

Dell Networking operating software 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.

debug dot1x

Display 802.1X debugging information.

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.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.4.1.0	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.

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

<i>vlan-id</i>	Enter the VLAN Identifier. The range is from 1 to 4094.
<i>max-attempts number</i>	(OPTIONAL) Enter the keywords <code>max-attempts</code> 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*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.



Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.12.0	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`).

Related Commands

- [dot1x port-control](#) — Enable port control on an interface
- [dot1x guest-vlan](#) — Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.
- [show dot1x interface](#) — Display the 802.1X configuration of an interface.

dot1x auth-server

Configure the authentication server to RADIUS.

Syntax `dot1x auth-server radius`

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
9.7(0.0)	Introduced on the S6000–ON.
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.
7.6.1.0	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.

Syntax	<code>dot1x auth-type mab-only</code>
Defaults	Disabled
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
8.4.2.1	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 <code>dot1x authentication</code> command). • Enable MAC authentication bypass on the port (the <code>dot1x mac-auth-bypass</code> 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.

Related Commands [dot1x mac-auth-bypass](#) — Enable MAC authentication bypass.

dot1x authentication (Configuration)

Enable dot1x globally. Enable dot1x both globally and at the interface level.

Syntax	<code>dot1x authentication</code> To disable dot1x on a globally, use the <code>no dot1x authentication</code> 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
9.7(0.0)	Introduced on the S6000–ON.
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.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series TeraScale.

Related Commands [dot1x authentication \(Interface\)](#) — Enables dot1x on an interface.

dot1x authentication (Interface)

Enable dot1x on an interface. Enable dot1x both globally and at the interface level.

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
9.7(0.0)	Introduced on the S6000–ON.
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.
7.6.1.0	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 guest-vlan

Configure a guest VLAN for limited access users or for devices that are not 802.1X capable.

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
9.7(0.0)	Introduced on the S6000–ON.
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.
7.6.1.0	Introduced on the C-Series, E-Series, and S-Series.

Usage Information 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.**

Related Commands

- [dot1x auth-fail-vlan](#) — Configure an authentication failure VLAN.
- [dot1x reauthentication](#) — Enable periodic re-authentication of the client.
- [dot1x reauth-max](#) —
Configure the maximum number of times to re-authenticate a port before it becomes unauthorized



dot1x host-mode

Enable single-host or multi-host authentication.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.
8.4.1.0	Added the <code>multi-auth</code> option on the C-Series and S-Series.
8.3.2.0	Added the <code>single-host</code> and <code>multi-host</code> 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.

Related Commands [show dot1x interface](#) — Display the 802.1X configuration of 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, Dell Networking OS attempts to authenticate the host based on its MAC address.

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

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.
9.0.2.0	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.
8.4.1.0	Introduced on the C-Series and S-Series.

Usage Information	To disable MAC authentication bypass on a port, enter the <code>no dot1x mac-auth-bypass</code> command.

dot1x max-eap-req

Configure the maximum number of times an extensive authentication protocol (EAP) request is transmitted before the session times out.

Syntax	<code>dot1x max-eap-req <i>number</i></code> To return to the default, use the <code>no dot1x max-eap-req</code> command.

Parameters	<i>number</i> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.



Version	Description
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-suplicants

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.

Syntax `dot1x max-suplicants 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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.
8.4.1.0	Introduced on the C-Series and S-Series.

Related Commands [dot1x host-mode](#) — Enables single-host or multi-host authentication.

dot1x port-control

Enable port control on an interface.

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 Auto

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.
7.6.1.0	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 you set `port-control` to `auto`.

dot1x quiet-period

Set the number of seconds that the authenticator remains quiet after a failed authentication with a client.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.



Version	Description
8.3.12.0	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 reauthentication of the client.

Syntax `dot1x reauthentication [interval seconds]`
 To disable periodic reauthentication, use the `no dot1x reauthentication` command.

Parameters

interval seconds	(Optional) Enter the keyword <code>interval</code> 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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.
7.6.1.0	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 re-authenticate before the port becomes unauthorized.

Syntax `dot1x reauth-max number`
 To return to the default, use the `no dot1x reauth-max` command.



Parameters	<i>number</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	
	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.
	9.0.2.0	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.
	7.6.1.0	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.

Syntax	<code>dot1x server-timeout seconds</code>									
	To return to the default, use the <code>no dot1x server-timeout</code> 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr></table>		Version	Description	9.7(0.0)	Introduced on the S6000–ON.	9.0.2.0	Introduced on the S6000.	9.0.0.0	Introduced on the Z9000.
Version	Description									
9.7(0.0)	Introduced on the S6000–ON.									
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.
8.3.12.0	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).

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 2/23/1
Dell(conf-if-te-2/23/1)#dot1x server-timeout 40
```

dot1x supplicant-timeout

Configure the amount of time after which exchanges with the supplicant time-out.

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
9.7(0.0)	Introduced on the S6000-ON.
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.

Version	Description
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.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.
7.6.1.0	Introduced on the C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

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.

Syntax `show dot1x cos-mapping interface interface [mac-address mac-address]`

Parameters **interface** Enter one of the following keywords and slot/port[/subport] or number 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.

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
9.7(0.0)	Introduced on the S6000–ON.
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.
8.4.2.1	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 tengigabitethernet 1/32/1

802.1p CoS re-map table on Te 1/32/1:

```
-----
Dot1p      Remapped Dot1p
0           7
1           6
2           5
3           4
4           3
5           2
6           1
7           0
Dell#
```

```
Dell#show dot1x cos-mapping interface tengigabitethernet 1/32/1 mac-
address 00:00:00:00:00:10
Supplicant Mac: 0 0 0 0 0 10 Lookup for Mac:
```

802.1p CoS re-map table on Te 1/32/1:

```
-----
```



802.1p CoS re-map table for Supplicant: 00:00:00:00:00:10

Dot1p	Remapped Dot1p
0	7
1	6
2	5
3	4
4	3
5	2
6	1
7	0

Dell#

show dot1x interface

Display the 802.1X configuration of an interface.

Syntax `show dot1x interface interface [mac-address mac-address]`

Parameters

<i>interface</i>	Enter one of the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
<i>mac-address</i>	(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
9.7(0.0)	Introduced on the S6000–ON.
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.
8.4.2.1	Added the <code>mac-address</code> 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) display for each supplicant, as shown in the following example.

Example

```
Dell#show dot1x interface tengigabitethernet 1/32/1

802.1x information on Te 1/32/1:
-----
Dot1x Status:          Enable
Port Control:          AUTO
Port Auth Status:      AUTHORIZED (MAC-AUTH-BYPASS)
Re-Authentication:     Disable
Untagged VLAN id:      400
Guest VLAN:            Enable
Guest VLAN id:         100
Auth-Fail VLAN:        Disable
Auth-Fail VLAN id:     NONE
Auth-Fail Max-Attempts: NONE
Mac-Auth-Bypass:       Enable
Mac-Auth-Bypass Only:  Enable
Tx Period:             3 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
Host Mode:             SINGLE_HOST
Auth PAE State:        Authenticated
Backend State:         Idle
Dell#
```

Example (mac-address)

```
Dell#show dot1x interface gigabitethernet 1/32 mac-address
00:00:00:00:00:10
Supplicant Mac: 0 0 0 0 0 10 Lookup for Mac:

802.1x information on Gi 1/32:
-----
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:       Enable
Mac-Auth-Bypass Only:  Enable
Tx Period:             3 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
Host Mode:             MULTI_AUTH
Max-Supplicants:       128

Port status and State info for Supplicant: 00:00:00:00:00:10

Port Auth Status:      AUTHORIZED (MAC-AUTH-BYPASS)
Untagged VLAN id:      400
Auth PAE State:        Authenticated
Backend State:         Idle
Dell#
```



```
Dell# show dot1x interface gigabitethernet 1/32 mac-address
00:00:00:00:00:11
Supplicant Mac: 0 0 0 0 0 10 Lookup for Mac:
```

```
802.1x information on Gi 1/32:
```

```
-----
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:       Enable
Mac-Auth-Bypass Only:  Enable
Tx Period:             3 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
Host Mode:             MULTI_AUTH
Max-Supplicants:       128
```

```
Port status and State info for Supplicant: 00:00:00:00:00:11
```

```
Port Auth Status:      AUTHORIZED(GUEST-VLAN)
Untagged VLAN id:      100
Auth PAE State:        Authenticated
Backend State:         Idle
Dell#
```

```
Dell#show dot1x interface tengigabitethernet 1/32/1 mac-address
00:00:00:00:00:10
Supplicant Mac: 0 0 0 0 0 10 Lookup for Mac:
```

```
802.1x information on Te 1/32/1:
```

```
-----
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:       Enable
Mac-Auth-Bypass Only:  Enable
Tx Period:             3 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
Host Mode:             MULTI_AUTH
Max-Supplicants:       128
```

```
Port status and State info for Supplicant: 00:00:00:00:00:10
```

```
Port Auth Status:      AUTHORIZED(MAC-AUTH-BYPASS)
Untagged VLAN id:      400
Auth PAE State:        Authenticated
Backend State:         Idle
Dell#
```

```
Dell# show dot1x interface tengigabitethernet 1/32/1 mac-address
```



00:00:00:00:00:11
Supplicant Mac: 0 0 0 0 0 10 Lookup for Mac:

802.1x information on Te 1/32/1:

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: Enable
Mac-Auth-Bypass Only: Enable
Tx Period: 3 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
Host Mode: MULTI_AUTH
Max-Supplicants: 128

Port status and State info for Supplicant: 00:00:00:00:00:11

Port Auth Status: AUTHORIZED(GUEST-VLAN)
Untagged VLAN id: 100
Auth PAE State: Authenticated
Backend State: Idle
Dell#



Access Control Lists (ACL)

Access control lists (ACLs) are supported by the Dell Networking OS.

Dell Networking OS supports the following types of ACL, IP prefix list, and route maps:

- Commands Common to all ACL Types
- Common IP ACL Commands
- Standard IP ACL Commands
- Extended IP ACL Commands
- Common MAC Access List Commands
- Standard MAC ACL Commands
- Extended MAC ACL Commands
- IP Prefix List Commands
- Route Map Commands
- AS-Path Commands
- IP Community List Commands

 **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 \(IPv6 ACLs\)](#).

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]`

Parameters

<i>remark-number</i>	Enter the remark number. The range is from 0 to 4294967290.

 **NOTE:** You can use the same sequence number for the remark and an ACL rule.

<i>description</i>	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, refer to the relevant *Dell 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.
9.0.2.0	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
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 4294967290 remarks in a given ACL.

The following example shows the use of the `remark` command twice within CONFIGURATION-STANDARD-ACCESS-LIST mode. The same sequence number was used for the remark and for an associated ACL rule. The remark precedes the rule in the running-config 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.

Example

```
Dell(config-std-nacl)#remark 10 Deny rest of the traffic
Dell(config-std-nacl)#remark 5 Permit traffic from XYZ Inc.
Dell(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
Dell(config-std-nacl)#
```

Related Commands [show config](#) — displays the current ACL configuration.

show config

Display the current ACL configuration.

Syntax `show config`

Command Modes

- CONFIGURATION-STANDARD-ACCESS-LIST
- CONFIGURATION-EXTENDED-ACCESS-LIST
- 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
9.7(0.0)	Introduced on the S6000–ON.
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.
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-std-nacl)#show conf
!
ip access-list standard test
 remark 5 Permit traffic from XYZ Inc.
 seq 5 permit 1.1.1.0/24 count
 remark 10 Deny traffic from ABC
 seq 10 deny 2.1.1.0/24 count
Dell(config-std-nacl)#
```

Common IP ACL Commands

The following commands are available within both Ingress and Egress 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 platform supports both Ingress and Egress IP ACLs.

 **NOTE:** Also refer to the [Commands Common to all ACL Types](#) section.

access-class

Apply a standard ACL to a terminal line.

Syntax

```
access-class access-list-name [ipv4 | ipv6]
```

To remove an ACL, use the `no access-class access-list-name [ipv4 | ipv6]` command.

Parameters

access-list-name	Enter the name of a configured Standard ACL, up to 140 characters.
ipv4	Enter the keyword <code>ipv4</code> to configure an IPv4 access class.
ipv6	Enter the keyword <code>ipv6</code> to configure an IPv6 access class.



Defaults	Not configured.
Command Modes	LINE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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

Version	Description
9.8(0.0)	Added the <code>ipv4</code> and <code>ipv6</code> parameters to the command. 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.
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.

Usage Information When you use the `access-class access-list-name` command without specifying the `ipv4` or `ipv6` attribute, both IPv4 as well as IPv6 rules that are defined in that ACL are applied to the terminal. This method is a generic way of configuring access restrictions.

To be able to filter access exclusively using either IPv4 or IPv6 rules, use either the `ipv4` or `ipv6` attribute along with the `access-class access-list-name` command. Depending on the attribute that you specify (`ipv4` or `ipv6`), the ACL processes either IPv4 or IPv6 rules, but not both. Using this configuration, you can set up two different types of access classes with each class processing either IPv4 or IPv6 rules separately.

However, if you already have configured generic IP ACL on a terminal line, then you cannot further apply IPv4 or IPv6 specific filtering on top of this configuration. Because, both IPv4 and IPv6 access classes are already configured on this terminal line. Before applying either IPv4 or IPv6 filtering, first undo the generic configuration using the `no access-class access-list-name` command.

Similarly, if you have configured either IPv4 or IPv6 specific filtering on a terminal line, you cannot apply generic IP ACLs on top of this configuration. Before applying the generic ACL configuration, first undo the existing configuration using the `no access-class access-list-name [ipv4 | ipv6]` command.

clear counters ip access-group

Erase all counters maintained for access lists.

Syntax `clear counters ip access-group [access-list-name]`



Parameters	<i>access-list-name</i> (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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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	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	<code>ip access-group <i>access-list-name</i> {in out} [implicit-permit] [vlan <i>vlan-id</i>] [vrf <i>vrf-name</i>]</code> To delete an IP access-group configuration, use the <code>no ip access-group <i>access-list-name</i> {in out} [implicit-permit] [vlan <i>vlan-id</i>] [vrf <i>vrf-name</i>]</code> command.

Parameters	<i>access-list-name</i> Enter the name of a configured access list, up to 140 characters.
	in Enter the keyword <code>in</code> to apply the ACL to incoming traffic.
	out Enter the keyword <code>out</code> to apply the ACL to outgoing traffic.
	implicit-permit (OPTIONAL) Enter the keyword <code>implicit-permit</code> 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 <i>vlan-id</i> (OPTIONAL) Enter the keyword <code>vlan</code> then the ID numbers of the VLANs. The range is from 1 to 4094 (you can use IDs from 1 to 4094).
	vrf <i>vrf-name</i> (OPTIONAL) Enter the keyword <code>vrf</code> 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.

Defaults Not enabled.

Command Modes INTERFACE/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
9.7(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.
8.1.1.0	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 You can assign one ACL (standard or extended 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.

Related Commands [ip access-list standard](#) — configures a standard ACL.

[ip access-list extended](#) — configures an extended ACL.

ip control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv4 CPU traffic.

Syntax `ip control-plane egress-filter`

Defaults	Not enabled.
Command Modes	EXEC Privilege
Command History	

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.

show ip accounting access-list

Display the IP access-lists created on the switch and the sequence of filters.

Syntax `show ip accounting {access-list access-list-name | cam_count} interface interface [vrf vrf-name]`

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 <code>interface</code> then the one of the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.
	in out	Identify whether ACL is applied on the ingress or egress side.
	vrf vrf-name	(Optional) Enter the keyword <code>vrf</code> and then the name of the VRF to view the IP accounting information on 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
9.0.2.0	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 the 4-port 40G line cards on ExaScale.



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.

Usage Information

<code>show ip accounting access-lists</code> Field	Description
"Extended IP..."	Displays the name of the IP ACL.
"seq 5..."	Displays the filter. If the keywords <code>count</code> or <code>byte</code> 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-list L3-ACL vrf vrf3
!
Standard Ingress IP access list L3-ACL on vrf3
Total cam count 3
seq 5 permit 10.1.2.0/24
  seq 10 permit 20.1.2.0/24
  seq 15 permit 30.1.2.0/24
Dell#
```

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 platform 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

To drop packets with a certain IP address, configure a filter.

Syntax `deny {source | any | host {ip-address}} [no-drop]`

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 in dotted decimal format of the network from which the packet was sent.
any	Enter the keyword <code>any</code> to specify that all routes are subject to the filter. You can enter any of the following keywords to specify route types.

- `bytes` — Enter the keyword `count` to count packets the filter processes.
- `count` — Enter the keyword `bytesorder` to count bytes the filter processes.
- `dscp` — Enter the keyword `dscp` followed by the DSCP value to match to the IP DSCP values. The range is from 0 to 63.
- `fragments` — Enter the keyword `fragments` to use ACLs to control packet fragments.
- `order` — Enter the keyword `order` to specify the QoS order of priority for the ACL entry. The range is from 0 to 254 (0 is the highest priority and 254 is the lowest; lower-order numbers have a higher priority). The default is, if you do not use the keyword `order`, the ACLs have the lowest order by default (255).

host <i>ip-address</i>	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address only.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the <code>no-drop</code> parameter.
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.
8.3.1.0	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 <code>monitor</code> option.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

The software cannot count both packets and bytes, so when you enter the `count` `byte` options, only bytes increment.

Related Commands [ip access-list standard](#) — configures a standard ACL.



[permit](#) — configures a permit filter.

ip access-list standard

Create a standard IP access list (IP ACL) to filter based on IP address.

Syntax	<code>ip access-list standard <i>access-list-name</i></code> To delete an access list, use the <code>no ip access-list standard <i>access-list-name</i></code> command.
Parameters	<i>access-list-name</i> 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.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	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.
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 <code>monitor</code> option.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information	Dell Networking OS supports one ingress and one egress IP ACL per interface. Prior to Dell Networking OS version 7.8.1.0, names are up to 16 characters long. The number of entries allowed per ACL is hardware-dependent. For detailed specifications on entries allowed per ACL, refer to your line card documentation.

Example	<pre>Dell(conf)#ip access-list standard TestList Dell(config-std-nacl)#</pre>

Related Commands	ip access-list extended — creates an extended access list. show config — displays the current configuration.



permit

To permit packets from a specific source IP address to leave the switch, configure a filter.

Syntax `permit {source [mask] | any | host ip-address} [no-drop]`

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 <code>any</code> to specify that all routes are subject to the filter. You can enter any of the following keywords to specify route types. • <code>bytes</code> — Enter the keyword <code>bytes</code> to count bytes processed by the filter. • <code>count</code> — Enter the keyword <code>count</code> to count packets the filter processes. • <code>dscp</code> — Enter the keyword <code>dscp</code> to match to the IP DSCP values. • <code>fragments</code> — Enter the keyword <code>fragments</code> to match to non-initial fragments of a datagram. • <code>order</code> — Enter the keyword <code>order</code> 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 <code>order</code>, the ACLs have the lowest order by default (255).
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address or hostname.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
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.
8.3.1.0	Add the DSCP value for ACL matching.



Version	Description
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 <code>monitor</code> option.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *Dell Networking OS 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 of an existing access-list.

Syntax `resequence access-list {ipv4 | ipv6 | mac} {access-list-name StartingSeqNum Step-to-Increment}`

Parameters

ipv4 ipv6 mac	Enter the keyword <code>ipv4</code> or <code>mac</code> to identify the access list type to resequence.
access-list-name	Enter the name of a configured IP access list.
StartingSeqNum	Enter the starting sequence number to resequence. The range is from 0 to 4294967290.
Step-to-Increment	Enter the step to increment the sequence number. The range is from 1 to 4294967290.

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
9.7(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.

Version	Description
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.

seq

Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

Syntax `seq sequence-number {deny | permit} {source [mask] | any | host ip-address}} [count [bytes]] [dscp value] [order] [fragments] [no-drop]`
 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 <code>deny</code> to configure a filter to drop packets meeting this condition.
permit	Enter the keyword <code>permit</code> 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 <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address or hostname.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
bytes	(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes the filter processes.
dscp	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
order	(OPTIONAL) Enter the keyword <code>order</code> 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 <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
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.
8.3.1.0	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 <code>monitor</code> option.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq sequence-number` command is applicable only in an ACL group.
- The `order` option works across ACL groups that are applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If you do not configure `sequence-number`, the rules with the same order value are ordered according to their configuration order.
- If you configure `sequence-number`, the sequence-number is used as a tie breaker for rules with the same order.

Related Commands [deny](#) — configures a filter to drop packets.
[permit](#) — configures a filter to forward packets.

Extended IP ACL Commands

When an ACL is created without any rule and then applied to an interface, ACL behavior reflects an implicit permit.

The following commands configure extended IP ACLs, which in addition to the IP address, also examine the packet's protocol type.

The platform 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.

Syntax

```
deny {ip | ip-protocol-number} {source mask | any | host ip-address}
{destination mask | any | host ip-address} [count [byte] | log] [dscp
value] [order] [monitor] [fragments] [no-drop]
```

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 <code>ip</code> to configure a generic IP access list. The keyword <code>ip</code> 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 <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> 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 <code>count</code> to count packets that the filter processes.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes that the filter processes.
log	(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to enter ACL matches in the log.
dscp	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
order	(OPTIONAL) Enter the keyword <code>order</code> 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 <code>order</code> , the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> 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 <i>Dell Networking OS Configuration Guide</i> .
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
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.
8.3.1.0	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 noncontiguous mask and added the <code>monitor</code> option.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS 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.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to the [Port Monitoring](#) chapter.

The C-Series and S-Series cannot count both packets and bytes, when you enter the count byte options, only bytes are incremented.



NOTE: When you configure ACL logging and byte counters simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

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.

Syntax

```
deny icmp {source mask | any | host ip-address} {destination mask | any |  
host ip-address} [dscp] [count [byte] [order] [fragments] [no-drop]
```

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 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 <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> 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.
dscp	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword <code>order</code> 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 <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the <code>no-drop</code> parameter.
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.
8.3.1.0	Added the keyword <code>dscp</code> .
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 non-contiguous mask and added the <code>monitor</code> option.



Version	Description
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to the [Port Monitoring](#) chapter.

deny tcp

Configure a filter that drops transmission control protocol (TCP) packets meeting the filter criteria.

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 [byte] [order] [fragments] [no-drop]
```

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 <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
dscp	Enter this keyword <code>dscp</code> to deny a packet based on the DSCP value. The range is from 0 to 63.
bit	Enter a flag or combination of bits: • <code>ack</code>: acknowledgement field • <code>fin</code>: finish (no more data from the user) • <code>psh</code>: push function • <code>rst</code>: reset the connection • <code>syn</code>: synchronize sequence numbers • <code>urg</code>: urgent field
operator	(OPTIONAL) Enter one of the following logical operand: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> 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 <code>count</code> to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
order	(OPTIONAL) Enter the keyword <code>order</code> 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 <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the <code>no-drop</code> parameter.
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.
8.3.1.0	Added the keyword <code>dscp</code> .
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 <code>monitor</code> option. Deprecated the keyword <code>established</code> .



Version	Description
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to the [Port Monitoring](#) chapter.

The C-Series and S-Series cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.

 **NOTE: When you configure ACL logging and byte counters 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	1111111111100000	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.

Syntax

```
deny udp {source mask | any | host ip-address} [operator port [port]]
{destination mask | any | host ip-address} [dscp] [operator port [port]]
[count [byte] [order] [fragments] [no-drop]
```

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 <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
dscp	Enter this keyword <code>dscp</code> 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: · <code>eq</code> = equal to · <code>neq</code> = not equal to · <code>gt</code> = greater than · <code>lt</code> = less than · <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> 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 <code>count</code> to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword <code>order</code> 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 <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the <code>no-drop</code> parameter.
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.
8.3.1.0	Added the keyword <code>dscp</code> .
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 <code>monitor</code> option. Deprecated the keyword <code>established</code> .
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the Quality of Service chapter of the *Dell Networking OS Configuration Guide*.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to the [Port Monitoring](#) chapter.

The C-Series and S-Series cannot count both packets and bytes; when you enter the count byte options, only bytes are incremented.



NOTE: When you configure ACL logging and byte counters 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	1111111111100000	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	1111111110000000	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

Name (or select) an extended IP access list (IP ACL) based on IP addresses or protocols.

Syntax `ip access-list extended access-list-name`
To delete an access list, use the `no ip access-list extended access-list-name` command.

Parameters ***access-list-name*** Enter a string up to 140 characters long as the access list name.

Defaults All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	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 specification about entries allowed per ACL, refer to your line card documentation.

Prior to 7.8.1.0, names are up to 16 characters long.

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.

Syntax `permit {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [bytes]] [dscp value] [order] [fragments] [no-drop]`

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 <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> 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 <code>count</code> to count packets processed by the filter.
bytes	(OPTIONAL) Enter the keyword <code>bytes</code> to count bytes processed by the filter.
dscp	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
order	(OPTIONAL) Enter the keyword <code>order</code> 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 <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
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.



Version	Description
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 <code>monitor</code> option.
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *Dell Networking OS Configuration Guide*.

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 tcp

To pass TCP packets meeting the filter criteria, configure a filter.

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 [byte] [order] [fragments] [no-drop]`

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 <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
bit	Enter a flag or combination of bits: • <code>ack</code>: acknowledgement field • <code>fin</code>: finish (no more data from the user) • <code>psh</code>: push function • <code>rst</code>: reset the connection • <code>syn</code>: 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.

byte (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 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.

no-drop Enter the keywords `no-drop` to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
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.



Version	Description
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the keyword <code>dscp</code> .
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 <code>monitor</code> option. Deprecated the keyword <code>established</code> .
6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information

The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *Dell Networking OS Configuration Guide*.



NOTE: When you configure ACL logging and byte counters simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.

The S-Series cannot count both packets and bytes; when you enter the count byte options, only bytes increment.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to [Port Monitoring](#).

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	1111111111100000	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	1111111110000000	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.

Syntax

```
permit udp {source mask | any | host ip-address} [operator port [port]]  
{destination mask | any | host ip-address} [dscp] [operator port [port]]  
[count [byte] [order] [fragments] [no-drop]
```

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 <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address.
dscp	Enter the keyword <code>dscp</code> 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: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> parameter)
port port	Enter the application layer port number. Enter two port numbers if you are using the <code>range</code> 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 <code>count</code> to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
order	(OPTIONAL) Enter the keyword <code>order</code> 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 <code>order</code> , the ACLs have the lowest order by default (255).
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
9.7(0.0)	Introduced on the S6000-ON.
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 <code>dscp</code> .
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 <code>monitor</code> option. .
6.5.1.0	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information The `order` option is relevant in the context of the Policy QoS feature only. For more information, refer to the “Quality of Service” chapter of the *Dell Networking OS Configuration Guide*.

 **NOTE: When you configure ACL logging and byte counters simultaneously, byte counters may display an incorrect value. Configure packet counters with logging instead.**

The S-Series cannot count both packets and bytes; when you enter the `count byte` options, only bytes increment.

The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to [Port Monitoring](#).

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	1111111111100000	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 access-list

Re-assign sequence numbers to entries of an existing access-list.

Syntax

```
resequence access-list {ipv4 | mac} {access-list-name StartingSeqNum Step-to-Increment}
```

Parameters

ipv4 mac	Enter the keyword <code>ipv4</code> or <code>mac</code> to identify the access list type to resequence.
access-list-name	Enter the name of a configured IP access list, up to 140 characters.
StartingSeqNum	Enter the starting sequence number to resequence. The range is from 0 to 4294967290.
Step-to-Increment	Enter the step to increment the sequence number. The range is from 1 to 4294967290.

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
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
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 all sequence numbers are exhausted, this feature permits re-assigning a new sequence number to entries of an existing access-list.

seq

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

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] | log] [dscp value] [order] [monitor] [fragments] [no-drop]`

Parameters	
sequence-number	Enter a number from 0 to 4294967290.
deny	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
permit	Enter the keyword <code>permit</code> 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 <code>icmp</code> to configure an ICMP access list filter.
ip	Enter the keyword <code>ip</code> to configure a generic IP access list. The keyword <code>ip</code> specifies that the access list permits all IP protocols.
tcp	Enter the keyword <code>tcp</code> to configure a TCP access list filter.
udp	Enter the keyword <code>udp</code> 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 <code>any</code> to specify that all routes are subject to the filter.
host ip-address	Enter the keyword <code>host</code> and then enter the IP address to specify a host IP address or hostname.
operator	(OPTIONAL) Enter one of the following logical operands: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> 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.
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
log	(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to enter ACL matches in the log. Supported on Jumbo-enabled line cards only.
dscp	(OPTIONAL) Enter the keyword <code>dscp</code> to match to the IP DSCP values.
order	(OPTIONAL) Enter the keyword <code>order</code> 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 <code>order</code> , the ACLs have the lowest order by default (255).
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> 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.
 NOTE: For more information, refer to the Flow-based Monitoring section in the Port Monitoring chapter of the <i>Dell Networking OS Configuration Guide</i> .	
fragments	Enter the keyword <code>fragments</code> to use ACLs to control packet fragments.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
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.
8.3.1.0	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.

Version	Description
7.4.1.0	Added support for the non-contiguous mask and added the <code>monitor</code> option. Deprecated the keyword <code>established</code> .
6.5.10	Expanded to include the optional QoS <code>order</code> priority for the ACL entry.

Usage Information The `monitor` option is relevant in the context of flow-based monitoring only. For more information, refer to [Port Monitoring](#).

The `order` option is relevant in the context of the Policy QoS feature only. The following applies:

- The `seq sequence-number` command is applicable only in an ACL group.
- The `order` option works across ACL groups that are applied on an interface via the QoS policy framework.
- The `order` option takes precedence over `seq sequence-number`.
- If you do not configure `sequence-number`, the rules with the same order value are ordered according to their configuration order.
- If you configure `sequence-number`, 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 details about 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.

If you configure the `sequence-number`, the `sequence-number` is used as a tie breaker for rules with the same order.



NOTE: When you configure ACL logging and byte counters 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.

Common MAC Access List 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 platform supports both Ingress and Egress MAC ACLs.

The MAC ACL can be applied on Physical, Port-channel and VLAN interfaces. As per the specified rules in the ACL, the traffic on the interface/ VLAN members or Port-channel members will be permitted or denied.

clear counters mac access-group

Clear counters for all or a specific MAC ACL.

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
9.7(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.
8.1.1.0	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.

mac access-group

Apply a MAC ACL to traffic entering or exiting an interface. The following interface types can be used for VLAN , Physical interface, Port channel interface. Enter into the interface mode and apply the `mac acl` in the following manner.

Syntax Applying MAC Access group on a physical / port channel interface
`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.

 **NOTE: The option is not available on the S-Series.**

**NOTE:**

1. If the MAC ACL is applied on VLAN, none of the VLAN members should have an access list applied for that VLAN.
2. If the MAC ACL is applied on a Physical or Port Channel interface, the VLAN in which this port is associated should not have an access list applied.
3. If the MAC ACL is applied on a VLAN, then that VLAN should not belong to VLAN ACL group.
4. If the MAC ACL is applied on a VLAN ACL group, then none of the VLANs in that group should have an access list applied on it.

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
9.7(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.
8.1.1.0	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.

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.

Syntax `show mac access-lists [access-list-name] [interface interface] [in | out]`

Parameters

access-list-name Enter the name of a configured MAC ACL, up to 140 characters.

interface interface Enter the keyword `interface` then the one of the following keywords and slot/port[/subport] or number 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 VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

in | out Identify whether ACL is applied on ingress or egress side.

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
9.7(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.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.4.1.0	Introduced.

show mac accounting access-list

Display MAC access list configurations and counters (if configured).

Syntax `show mac accounting access-list access-list-name interface interface in | out`

Parameters

- access-list-name*** Enter the name of a configured MAC ACL, up to 140 characters.
- interface interface*** Enter the keyword `interface` then the one of the following keywords and slot/port[/subport] or number 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.

in | out Identify whether ACL is applied on 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
9.7(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.
8.5.1.0	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

The ACL hit counters increment the counters for each matching rule, not just the first matching rule.

Example

```
Dell#show mac accounting access-list TestMac interface tengigabitethernet
1/8/1 in
Ingress Standard mac access-list TestMac on TenGigabitEthernet 1/89/1
Total cam count 2
  seq 5 permit aa:aa:aa:aa:00:00 00:00:00:00:ff:ff count (0 packets)
  seq 10 deny any count (20072594 packets)
Dell#
```

Standard MAC ACL Commands

When you create an access control list without any rule and then apply it to an interface, the ACL behavior reflects implicit permit. These commands configure standard MAC ACLs and support both Ingress and Egress MAC ACLs.

 **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 the MAC address specified, configure a filter.

Syntax

```
deny {any | mac-source-address [mac-source-address-mask]} [count [byte]]
[log] [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 <code>any</code> to specify that all routes are subject to the filter.
mac-source-address	Enter a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
mac-source-address-mask	(OPTIONAL) Specify which bits in the MAC address must match. If no mask is specified, a mask of <code>00:00:00:00:00:00</code> is applied (in other words, the filter allows only MAC addresses that match).
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
log	(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to log the packets.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> 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 <i>Dell Networking OS Configuration Guide</i> .

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
9.7(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.
8.1.1.0	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 <code>monitor</code> 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 packets' details.



NOTE: When you configure ACL logging and byte counters 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.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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	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 Dell Networking OS supports one ingress and one egress MAC ACL per interface.

The number of entries allowed per ACL is hardware-dependent. For detailed specifications about entries allowed per ACL, refer to your line card documentation.

 **NOTE: Ingress ACLs are supported on C-Series and S-Series platforms only.**

Example

```
Dell(conf)#mac-access-list access-list standard TestMAC
Dell(config-std-macl)#permit 00:00:00:00:00:00 00:00:00:00:ff:ff count
Dell(config-std-macl)#deny any count
```



permit

To forward packets from a specific source MAC address, configure a filter.

Syntax `permit {any | mac-source-address [mac-source-address-mask]} [count [byte]]
| [log] [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 <code>any</code> 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 <code>count</code> to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
log	(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to log the packets.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> 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.



NOTE: 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
9.7(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.
8.1.1.0	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.

Usage Information When you use the `log` option, the CP processor logs details about 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.



NOTE: When you configure the ACL logging and byte counters 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.

Syntax `seq sequence-number {deny | permit} {any | mac-source-address [mac-source-address-mask]} [count [byte]] [log] [monitor] [no-drop]`
To remove this filter, use the `no seq sequence-number` command.

Parameters

<i>sequence-number</i>	Enter a number from 0 to 65535.
<i>deny</i>	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
<i>permit</i>	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this criteria.
<i>any</i>	Enter the keyword <code>any</code> to filter all packets.
<i>mac-source-address</i>	Enter a MAC address in nn:nn:nn:nn:nn:nn format.
<i>mac-source-address-mask</i>	(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).
<i>count</i>	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
<i>byte</i>	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
<i>log</i>	(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to log the packets.
<i>monitor</i>	(OPTIONAL) Enter the keyword <code>monitor</code> 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.



NOTE: For more information, refer to the “Flow-based Monitoring” section in the Port Monitoring chapter of the *Dell Networking OS Configuration Guide*.

no-drop Enter the keywords `no-drop` to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
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.
8.1.1.0	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 <code>monitor</code> option.
6.1.1.0	Introduced on the E-Series.

Usage Information When you use the `log` option, the CP processor logs details about 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.



NOTE: When you configure the ACL logging and byte counters 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

When an access-list is created without any rule and then applied to an interface, ACL behavior reflects implicit permit. The following commands configure Extended MAC ACLs.

The platform supports both Ingress and Egress MAC ACLs.



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.

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] [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 <code>any</code> to drop all packets.
host <i>mac-address</i>	Enter the keyword <code>host</code> and then enter a MAC address to drop packets with that host address.
<i>mac-source-address</i>	Enter a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
<i>mac-source-address-mask</i>	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of <code>ff:ff:ff:ff:ff:ff</code> allows entries that do not match and a mask of <code>00:00:00:00:00:00</code> only allows entries that match exactly.
<i>mac-destination-address</i>	Enter the destination MAC address and mask in <code>nn:nn:nn:nn:nn:nn</code> format.
<i>mac-destination-address-mask</i>	Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of <code>ff:ff:ff:ff:ff:ff</code> allows entries that do not match and a mask of <code>00:00:00:00:00:00</code> only allows entries that match exactly.
<i>ethertype operator</i>	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • <code>ev2</code> - is the Ethernet II frame format • <code>llc</code> - is the IEEE 802.3 frame format • <code>snap</code> - is the IEEE 802.3 SNAP frame format
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets processed by the filter.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes processed by the filter.
log	(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to log the packets.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> 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 <i>Dell Networking OS Configuration Guide</i> .



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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Added the <code>monitor</code> option.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </tbody> </table>	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.	8.1.1.0	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 <code>monitor</code> option.	6.1.1.0	Introduced on the E-Series.
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.																						
8.1.1.0	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 <code>monitor</code> option.																						
6.1.1.0	Introduced on the E-Series.																						
Usage Information	When you use the <code>log</code> 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.  NOTE: When you configure the ACL logging and byte counters 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

Name a new or existing extended MAC access control list (extended MAC ACL).

Syntax	<pre>mac access-list extended <i>access-list-name</i> [cpu-qos</pre> To delete a MAC access list, use the <code>no mac access-list extended <i>access-list-name</i></code> command.	
Parameters	<i>access-list-name</i> Enter a text string as the MAC access list name, up to 140 characters. cpu-qos Enter the keywords <code>cpu-qos</code> to assign this ACL to control plane traffic only (CoPP).	
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
9.7(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.
8.3.10.0	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 about entries allowed per ACL, refer to your line card documentation.

Prior to 7.8.1.0, names are up to 16 characters long.

Example

```
Dell(config)#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(config)#do show mac accounting access-list snickers interface tengig
1/17 in
Extended mac access-list snickers on TenGigabitEthernet 1/17
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.

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] [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 <code>any</code> to forward all packets.
host	Enter the keyword <code>host</code> then a MAC address to forward packets with that host address.
<i>mac-source-address</i>	Enter a MAC address in <code>nn:nn:nn:nn:nn:nn</code> format.
<i>mac-source-address-mask</i>	(OPTIONAL) Specify which bits in the MAC address must match. The MAC ACL supports an inverse mask; therefore, a mask of <code>ff:ff:ff:ff:ff:ff</code> allows entries that do not match and a mask of <code>00:00:00:00:00:00</code> only allows entries that match exactly.
<i>mac-destination-address</i>	Enter the destination MAC address and mask in <code>nn:nn:nn:nn:nn:nn</code> format.
<i>mac-destination-address-mask</i>	Specify which bits in the MAC address must be matched. The MAC ACL supports an inverse mask; therefore, a mask of <code>ff:ff:ff:ff:ff:ff</code> allows entries that do not match and a mask of <code>00:00:00:00:00:00</code> only allows entries that match exactly.
<i>ethertype operator</i>	(OPTIONAL) To filter based on protocol type, enter one of the following Ethertypes: • <code>ev2</code> - is the Ethernet II frame format • <code>llc</code> - is the IEEE 802.3 frame format • <code>snap</code> - is the IEEE 802.3 SNAP frame format
count	(OPTIONAL) Enter the keyword <code>count</code> to count packets the filter processes.
byte	(OPTIONAL) Enter the keyword <code>byte</code> to count bytes the filter processes.
log	(OPTIONAL, E-Series only) Enter the keyword <code>log</code> to log the packets.
monitor	(OPTIONAL) Enter the keyword <code>monitor</code> 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.





NOTE: 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
9.7(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.
8.1.1.0	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 <code>monitor</code> option.
6.1.1.0	Introduced on the E-Series.

Usage Information When you use the `log` option, the CP processor logs details about 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.



NOTE: When you configure the ACL logging and byte counters 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.

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.

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
9.7(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.
8.1.1.0	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.

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

<i>ip-prefix</i>	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.
<i>ge min-prefix-length</i>	(OPTIONAL) Enter the keyword <code>ge</code> and then enter the minimum prefix length, which is a number from zero (0) to 32.
<i>le max-prefix-length</i>	(OPTIONAL) Enter the keyword <code>le</code> 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
9.7(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.
8.1.1.0	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.

ip prefix-list

Enter the PREFIX-LIST mode and configure a prefix list.

Syntax `ip prefix-list prefix-name`

To delete a prefix list, use the `no ip prefix-list prefix-name` command.

Parameters

<i>prefix-name</i>	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
9.7(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.
8.1.1.0	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.
6.2.1.1	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.

seq

To a deny or permit filter in a prefix list while configuring the filter, assign a sequence number.

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 4294967294.
deny	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition..
permit	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this condition.
any	(OPTIONAL) Enter the keyword <code>any</code> 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 <code>ge</code> and then enter the minimum prefix length, which is a number from zero (0) to 32.
le max-prefix-length	(OPTIONAL) Enter the keyword <code>le</code> and then enter the maximum prefix length, which is a number from zero (0) to 32.
bitmask number	Enter the keyword <code>bitmask</code> 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
9.7(0.0)	Introduced on the S6000–ON.
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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.3.1.0	Added the <code>bit mask</code> option.

Usage Information If you do not use the `ge` or `le` options, only packets with an exact match to the prefix are filtered.

show config

Display the current PREFIX-LIST configurations.

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
9.7(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.
8.1.1.0	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-nprefix1)#show config
!
ip prefix-list snickers
Dell(conf-nprefix1)#
```

show ip prefix-list detail

Display details of the configured prefix lists.

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
9.7(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.
8.1.1.0	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
Ip Prefix-list with the last deletion/insertion: PL_OSPF_to_RIP
ip prefix-list PL_OSPF_to_RIP:
count: 3, range entries: 1, sequences: 5 - 25
  seq 5 permit 1.1.1.0/24 (hit count: 0)
  seq 10 deny 2.1.0.0/16 ge 23 (hit count: 0)
  seq 25 permit 192.0.0.0 bitmask 192.0.0.0 (hit count: 800)
```

show ip prefix-list summary

Display a summary of the configured prefix lists.

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
9.7(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.
8.1.1.0	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 summary
Ip Prefix-list with the last deletion/insertion: PL_OSPF_to_RIP
ip prefix-list PL_OSPF_to_RIP:
count: 3, range entries: 1, sequences: 5 - 25
```

Route Map Commands

When you create an access-list without any rule and then applied 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.

Syntax	<code>continue [sequence-number]</code>
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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
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 configured, 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.

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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
pre-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.

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
9.7(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.
8.1.1.0	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.
pre-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.

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 <code>exact</code> 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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

Related Commands [set community](#) — specifies a COMMUNITY attribute.

match interface

To match routes whose next hop is on the interface specified, configure a filter.

Syntax `match interface interface`
 To remove a match, use the `no match interface interface` command.



Parameters

interface

Enter the following keywords and slot/port[/subport] or number 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. The range is from 1 to 128.
- For a VLAN interface, enter the keyword `vlan` then a number from 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
9.7(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.
8.5.1.0	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.

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
9.7(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.
8.1.1.0	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.
pre-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.

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 <code>prefix-list</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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	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.
pre-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.

Syntax	<code>match ip route-source {prefix-list prefix-list-name}</code> To delete a match, use the <code>no match ip route-source {prefix-list prefix-list-name}</code> 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
9.7(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
8.1.1.0	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.
pre-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.

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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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.

Syntax `match origin {egp | igp | incomplete}`

To disable matching filter, use the `no match origin {igp | egp | incomplete}` command.

Parameters	egp	Enter the keyword <code>egp</code> to match routes originating outside the AS.
	igp	Enter the keyword <code>igp</code> to match routes originating within the same AS.
	incomplete	Enter the keyword <code>incomplete</code> 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 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.
9.0.2.0	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.
pre-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.

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 <code>external</code> then either <code>type-1</code> or <code>type-2</code> to match only on OSPF Type 1 routes or OSPF Type 2 routes.
internal	Enter the keyword <code>internal</code> to match only on routes generated within OSPF areas.
level-1	Enter the keyword <code>level-1</code> to match IS-IS Level 1 routes.
level-2	Enter the keyword <code>level-2</code> to match IS-IS Level 2 routes.
local	Enter the keyword <code>local</code> 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
9.7(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.
8.1.1.0	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.
pre-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.

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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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.

Syntax	<code>route-map <i>map-name</i> [permit deny] [<i>sequence-number</i>]</code> To delete a route map, use the <code>no route-map <i>map-name</i> [permit deny] [<i>sequence-number</i>]</code> command.	
Parameters	<i>map-name</i>	Enter a text string of up to 140 characters to name the route map for easy identification.
	<i>permit</i>	(OPTIONAL) Enter the keyword <code>permit</code> to set the route map default as permit. If you do not specify a keyword, the default is <code>permit</code> .
	<i>deny</i>	(OPTIONAL) Enter the keyword <code>deny</code> to set the route map default as deny.
	<i>sequence-number</i>	(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 (<code>permit</code> or <code>deny</code>) for the route map, the <code>permit</code> action is the default.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	



Version	Description
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 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(config)#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.

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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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.

set automatic-tag

To automatically compute the tag value of the route, configure a filter.

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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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.

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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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	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.
pre-6.1.1.0	Introduced on the E-Series.

Usage Information	The community list used in the <code>set comm-list delete</code> command must be configured so that each filter contains only one community. For example, the filter <code>deny 100:12</code> is acceptable, but the filter <code>deny 120:13 140:33</code> 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	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.

Syntax	<code>set community {community-number local-as no-advertise no-export none} [additive]</code> To delete a BGP COMMUNITY attribute assignment, use the <code>no set community {community-number local-as no-advertise no-export none}</code> 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 <code>local-as</code> to drop all routes with the COMMUNITY attribute of <code>NO_EXPORT_SUBCONFED</code> .



All routes with the NO_EXPORT_SUBCONFED (0xFFFFFFFF03) community attribute must not be advertised to external BGP peers.

no-advertise	Enter the keywords <code>no-advertise</code> to drop all routes containing the well-known community attribute of NO_ADVERTISE. All routes with the NO_ADVERTISE (0xFFFFFFFF02) community attribute must not be advertised to other BGP peers.
no-export	Enter the keywords <code>no-export</code> to drop all routes containing the well-known community attribute of NO_EXPORT. All routes with the NO_EXPORT (0xFFFFFFFF01) community attribute must not be advertised outside a BGP confederation boundary.
none	Enter the keyword <code>none</code> to remove the community attribute from routes meeting the route map criteria.
additive	(OPTIONAL) Enter the keyword <code>additive</code> 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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

Related Commands [match community](#) — redistributes routes that match the COMMUNITY attribute.

set level

To specify the IS-IS level or OSPF area to which matched routes are redistributed, configure a filter.

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 <code>backbone</code> to redistribute matched routes to the OSPF backbone area (area 0.0.0.0).
	level-1	Enter the keyword <code>level-1</code> to redistribute matched routes to IS-IS Level 1.
	level-1-2	Enter the keyword <code>level-1-2</code> to redistribute matched routes to IS-IS Level 1 and Level 2.
	level-2	Enter the keyword <code>level-2</code> to redistribute matched routes to IS-IS Level 2.
	stub-area	Enter the keyword <code>stub</code> 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 Dell Networking OS 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.
9.0.2.0	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

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.

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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
7.6.1.0	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	The <code>set local-preference</code> command changes the LOCAL_PREF attribute for routes meeting the route map criteria. To change the LOCAL_PREF for all routes, use the <code>bgp default local-preference</code> 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.

Syntax	<code>set metric [+ -] metric-value</code> To delete a setting, enter <code>no set metric</code> .

Parameters	+	(OPTIONAL) Enter + to add a metric-value to the redistributed routes.
	-	(OPTIONAL) Enter – to subtract a metric-value from the redistributed routes.
	<i>metric-value</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.



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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

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.

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 <code>internal</code> 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 <code>external</code> to assign the IS-IS external metric.
	type-1	Enter the keyword <code>type-1</code> to assign the OSPF Type 1 metric.
	type-2	Enter the keyword <code>type-2</code> 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
9.7(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	Implemented the keyword <code>internal</code> .
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.
pre-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.

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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.



Usage Information	If you configure the <code>set next-hop</code> command, its configuration takes precedence over the <code>neighbor next-hop-self</code> command in the ROUTER BGP mode. If you configure the <code>set next-hop</code> 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.

Syntax	<pre>set origin {igp egp incomplete}</pre> To delete an ORIGIN attribute setting, use the <code>no set origin</code> command.						
Parameters	<table> <tr> <td>egp</td><td>Enter the keyword <code>egp</code> to set routes originating from outside the local AS.</td></tr> <tr> <td>igp</td><td>Enter the keyword <code>igp</code> to set routes originating within the same AS.</td></tr> <tr> <td>incomplete</td><td>Enter the keyword <code>incomplete</code> to set routes with incomplete routing information.</td></tr> </table>	egp	Enter the keyword <code>egp</code> to set routes originating from outside the local AS.	igp	Enter the keyword <code>igp</code> to set routes originating within the same AS.	incomplete	Enter the keyword <code>incomplete</code> to set routes with incomplete routing information.
egp	Enter the keyword <code>egp</code> to set routes originating from outside the local AS.						
igp	Enter the keyword <code>igp</code> to set routes originating within the same AS.						
incomplete	Enter the keyword <code>incomplete</code> 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 <i>Dell Networking OS Command Line Reference Guide</i>.						

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.
9.0.2.0	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

set tag

To specify a tag for redistributed routes, configure a filter.

Syntax	<code>set tag tag-value</code>



To delete a setting, use the `no set tag` command.

Parameters	<i>tag-value</i> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

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.

Syntax	<code>set weight weight</code> To delete a weight specification, use the <code>no set weight weight</code> command.

Parameters	<i>weight</i> 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>pre-6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </tbody> </table>	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.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	pre-6.1.1.0	Introduced on the E-Series.
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.																				
8.1.1.0	Introduced on the E-Series ExaScale.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
pre-6.1.1.0	Introduced on the E-Series.																				
Usage Information	If you do not use the <code>set weight</code> 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.

Syntax	<code>show config</code>																				
Command Modes	ROUTE-MAP																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>pre-6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </tbody> </table>	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.	8.1.1.0	Introduced on the E-Series ExaScale.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	pre-6.1.1.0	Introduced on the E-Series.
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.																				
8.1.1.0	Introduced on the E-Series ExaScale.																				
7.6.1.0	Introduced on the S-Series.																				
7.5.1.0	Introduced on the C-Series.																				
pre-6.1.1.0	Introduced on the E-Series.																				



Example

```
Dell(conf-nprefix1)#show config
!
ip prefix-list PL_OSPF_to_RIP
 seq 5 permit 1.1.1.0/24
 seq 10 deny 2.1.0.0/16 ge 23
 seq 25 permit 192.0.0.0 bitmask 192.0.0.0
```

show route-map

Display the current route map configurations.

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
97(0.0)	Introduced on the S6000–ON.
90.2.0	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	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.
pre-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.

deny (for Standard IP ACLs)

To drop packets with a certain IP address, configure a filter.

Syntax `deny {source | 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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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

CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
9.3(0.0)	Added support for logging of ACLs on the S4810, S4820T, and Z9000 platforms.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, 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 [ip access-list standard](#) — configures a standard ACL.

[permit](#) — configures a permit filter.

deny (for Extended IP ACLs)

Configure a filter that drops IP packets meeting the filter criteria.

Syntax `deny {ip | ip-protocol-number} {source mask | any | host ip-address} {destination mask | any | host ip-address} [count [byte]] [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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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 CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.



Version	Description
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

[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.

seq (for Standard IPv4 ACLs)

Assign a sequence number to a deny or permit filter in an IP access list while creating the filter.

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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 [deny](#) — Configures a filter to drop packets.

[permit](#) — Configures a filter to forward packets.

deny tcp (for Extended IP ACLs)

Configure a filter that drops transmission control protocol (TCP) packets meeting the filter criteria.

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 [byte]] [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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Added the support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0)	Added the 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 [deny](#) — assigns a filter to deny IP traffic.

[deny udp](#) — assigns a filter to deny UDP traffic.

deny ether-type (for Extended MAC ACLs)

Configure an egress filter that drops specified types of Ethernet packets on egress ACL supported line cards. (For more information, refer to your line card documentation).

Syntax `deny ether-type protocol-type-number {destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-address mac-address-mask | any} [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 ether-type protocol-type-number {destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-address mac-address-mask | any}` command.

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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 CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.



Version	Description
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 (for Standard MAC ACLs)

To drop packets with a the MAC address specified, configure a filter.

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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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 CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
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](#) — configures a MAC address filter to pass packets.

[seq](#) — configures a MAC address filter with a specified sequence number.

deny (for Extended MAC ACLs)

To drop packets that match the filter criteria, configure a filter.

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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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

CONFIGURATION-MAC ACCESS LIST-EXTENDED

Command History

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
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](#) — configures a MAC address filter to pass packets.

[seq](#) — configures a MAC address filter with a specified sequence number.

permit (for Standard IP ACLs)

To permit packets from a specific source IP address to leave the switch, configure a filter.

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	log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
	threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
	interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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 CONFIGURATION-STANDARD-ACCESS-LIST

Command History	Version	Description
	9.7(0.0)	Introduced on the S6000–ON.
	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 [deny](#) — Assigns a IP ACL filter to deny IP packets.

[ip access-list standard](#) — Creates a standard ACL.

permit arp (for Extended MAC ACLs)

Configure a filter that forwards ARP packets meeting this criteria. This command is supported only on 12-port GE line cards with SFP optics; refer to your line card documentation for specifications.

Syntax `permit arp {destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number} [count [byte]] [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 `{destination-mac-address mac-address-mask | any} vlan vlan-id {ip-address | any | opcode code-number}` command.

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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 CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 ether-type (for Extended MAC ACLs)

Configure a filter that allows traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics. For specifications, refer to your line card documentation.

Syntax

```
permit ether-type protocol-type-number {destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-address mac-address-mask | any} [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 permit ether-type protocol-type-number {destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-address mac-address-mask | any} command`.

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <i>minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 Extended IP ACLs)

Configure a filter to allow all or specific ICMP messages.

Syntax

```
permit icmp {source mask | any | host ip-address} {destination mask | any |  
host ip-address} [dscp] [message-type] [count [byte]] [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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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

CONFIGURATION-STANDARD-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
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 udp (for Extended IP ACLs)

To pass UDP packets meeting the filter criteria, configure a filter.

Syntax

```
permit udp {source mask | any | host ip-address} [operator port [port]]  
{destination mask | any | host ip-address} [dscp] [operator port [port]]  
[count [byte]] [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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 [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.

permit (for Extended IP ACLs)

To pass IP packets meeting the filter criteria, configure a filter.

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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in-msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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 CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
9.4(0.0)	Added the support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.
9.3(0.0)	Added the 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, standard and extended IPv6 ACLs, and standard and extended 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

- [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 (for Standard MAC ACLs)

To forward packets from a specific source MAC address, configure a filter.

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

log (OPTIONAL) Enter the keyword `log` to enable the triggering of ACL log messages.



threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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 History

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
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

[deny](#) — configures a MAC ACL filter to drop packets.

[seq](#) —configure a MAC ACL filter with a specified sequence number.

seq (for Standard MAC ACLs)

To a deny or permit filter in a MAC access list while creating the filter, assign a sequence number.

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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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

CONFIGURATION-MAC ACCESS LIST-STANDARD

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 [deny](#) — configures a filter to drop packets.

[permit](#) — configures a filter to forward packets.

permit tcp (for Extended IP ACLs)

To pass TCP packets meeting the filter criteria, configure a filter.

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 [byte]] [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 tcp {source mask | any | host ip-address} {destination mask | any | host ip-address}` command.

Parameters	log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
	threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
	interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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 CONFIGURATION-EXTENDED-ACCESS-LIST

Command History	Version	Description
	9.7(0.0)	Introduced on the S6000–ON.
	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

[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.

seq arp (for Extended MAC ACLs)

Configure an egress filter with a sequence number that filters ARP packets meeting this criteria. This command is supported only on 12-port GE line cards with SFP optics. For specifications, refer to your line card documentation.

 **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

```
seq sequence-number {deny | permit} 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, use the `no seq sequence-number` command.

Parameters

<code>log</code>	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
<code>threshold-in msgs count</code>	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. You can enter a threshold in the range of 1-100.
<code>interval minutes</code>	(OPTIONAL) Enter the keyword <code>interval</code> 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 CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 reenabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is reenabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, standard and extended IPv6 ACLs, and standard and extended 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).

seq ether-type (for Extended MAC ACLs)

Configure an egress filter with a specific sequence number that filters traffic with specified types of Ethernet packets. This command is supported only on 12-port GE line cards with SFP optics. For specifications, refer to your line card documentation.

 **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 `seq sequence-number {deny | permit} ether-type protocol-type-number
{destination-mac-address mac-address-mask | any} vlan vlan-id {source-mac-`


```
address mac-address-mask | any} [count [byte]] [order] [log [interval
minutes] [threshold-in-msgs [count]] [monitor]
```

To remove this filter, use the `no seq sequence-number` command.

Parameters

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. You can enter a threshold in the range of 1-100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 reenabled for this new interval.

If ACL logging is stopped because the configured threshold is exceeded, it is reenabled after the logging interval period elapses. ACL logging is supported for standard and extended IPv4 ACLs, standard and extended IPv6 ACLs, and standard and extended 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).

seq (for IP ACLs)

Assign a sequence number to a deny or permit filter in an extended IP access list while creating the filter.

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

log	(OPTIONAL) Enter the keyword <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100..
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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 CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
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 [deny](#) — configures a filter to drop packets.

[permit](#) — configures a filter to forward 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.

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 <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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
9.7(0.0)	Introduced on the S6000–ON.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.



Version	Description
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](#) – configures a filter to forward packets.

permit udp (for IPv6 ACLs)

Configure a filter to pass UDP packets meeting the filter criteria.

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 <code>log</code> to enable the triggering of ACL log messages.
	threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
	interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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
9.7(0.0)	Introduced on the S6000–ON.
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](#) – assigns a permit filter for IP packets.

permit tcp (for IPv6 ACLs)

Configure a filter to pass TCP packets that match the filter criteria.

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 <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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](#) – assigns a permit filter for IP packets.

permit icmp (for IPv6 ACLs)

To allow all or specific internet control message protocol (ICMP) messages, configure a filter.

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 <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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
9.7(0.0)	Introduced on the S6000–ON.
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 (for IPv6 ACLs)

To configure a filter that matches the filter criteria, select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP.

Syntax `permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]]] [monitor] [no-drop]`

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 <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
9.7(0.0)	Introduced on the S6000–ON.
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.

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 <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.



interval <i>minutes</i>	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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
9.7(0.0)	Introduced on the S6000–ON.
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).



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).

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 <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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

CONFIGURATION-EXTENDED-ACCESS-LIST

Command History

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
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.

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 <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100..
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Added support for flow-based monitoring on the S4810, S4820T, S6000, and Z9000 platforms.



Version	Description
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.

 **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 <code>log</code> to enable the triggering of ACL log messages.
	threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. You can enter a threshold in the range of 1-100.
	interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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
9.7(0.0)	Introduced on the S6000–ON.
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 (for IPv6 ACLs)

Configure a filter that drops IPv6 packets that match the filter criteria.

Syntax `deny {ipv6-protocol-number | icmp | ipv6 | tcp | udp} [count [byte]] [dscp value] [order] [fragments] [log [interval minutes] [threshold-in-msgs [count]]] [monitor] [no-drop]`

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 <code>log</code> to enable the triggering of ACL log messages.
threshold-in msgs count	(OPTIONAL) Enter the <code>threshold-in-msgs</code> 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 <code>seq</code> , <code>permit</code> , or <code>deny</code> commands. The threshold range is from 1 to 100.
interval minutes	(OPTIONAL) Enter the keyword <code>interval</code> 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 <code>monitor</code> 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.
no-drop	Enter the keywords <code>no-drop</code> to match only the forwarded packets.

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
9.8(0.0)	Added the no-drop parameter.
9.7(0.0)	Introduced on the S6000-ON.
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).



Bidirectional Forwarding Detection (BFD)

Bidirectional forwarding detection (BFD) is a detection protocol that provides fast forwarding path failure detection.

The Dell Networking operating software implementation is based on the standards specified in the IETF Draft draft-ietf-bfd-base-03 and supports BFD on all Layer 3 physical interfaces including VLAN interfaces and port-channels

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.

Syntax	<code>bfd all-neighbors [interval <i>interval</i> min_rx <i>min_rx</i> multiplier <i>value</i> role {active passive}]</code>	
Parameters	interval <i>milliseconds</i>	(OPTIONAL) Enter the keyword <code>interval</code> to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 100 .
	min_rx <i>milliseconds</i>	Enter the keyword <code>min_rx</code> 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 100. The default is 100 .
	multiplier <i>value</i>	Enter the keyword <code>multiplier</code> 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 <i>Parameters</i> .	
Command Modes	ROUTER OSPF	
	ROUTER OSPFv3	
	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
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
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 timer values configured with the `bfd neighbor` command 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 neighbor` 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 neighbor` command or configured for the peer group to which a neighbor belongs. The neighbors inherit only the global timer values (configured with the `bfd neighbor` command).

You can only enable BFD for VRRP in INTERFACE command mode (`vrrp bfd all-neighbors`).

Related Commands

[neighbor bfd disable](#) — Explicitly disables a BFD session with a BGP neighbor or a BGP peer group.

ip route bfd

Enable BFD for all neighbors configured through static routes.

Syntax

```
ip route bfd [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 [interval interval min_rx min_rx multiplier value role {active | passive}]` command.

Parameters

interval <i>milliseconds</i>	(OPTIONAL) Enter the keywords <code>interval</code> to specify non-default BFD session parameters beginning with the transmission interval. The range is from 50 to 1000. The default is 100 .
min_rx <i>milliseconds</i>	Enter the keywords <code>min_rx</code> 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 100 .
multiplier <i>value</i>	Enter the keywords <code>multiplier</code> 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

CONFIGURATION

Command History

Version	Description
9.7(0.0)	Introduced on the S6000–ON.
9.3(0.0)	Introduced on S6000.
9.2(0.0)	Introduced on Z9000, S4810, and S4820T.
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.

neighbor bfd

Explicitly enable a BFD session with a BGP neighbor or a BGP peer group.

Syntax

`neighbor {ip-address | peer-group-name} bfd`

Parameters

<i>ip-address</i>	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
9.7(0.0)	Introduced on the S6000–ON.
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.
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 neighbor` command, the default BFD session parameters are used (interval: **100** milliseconds, min_rx: **100** milliseconds, multiplier: **3** packets, and role: **active**) if you have not specified parameters with the `bfd neighbor` 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 neighbor` command or configured for the peer group to which the neighbor belongs.
- The neighbor only inherits the global timer values configured with the `bfd neighbor` 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.

neighbor bfd disable

Explicitly disable a BFD session with a BGP neighbor or a BGP peer group.

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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
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 <code>neighbor bfd disable</code> command: • The neighbor does not inherit the global BFD disable values configured with the <code>bfd neighbor</code> command or configured for the peer group to which the neighbor belongs. • The neighbor only inherits the global timer values configured with the <code>bfd neighbor</code> command: <code>interval</code>, <code>min_rx</code>, and <code>multiplier</code>.

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 neighbor` command or configured for the peer group to which the neighbor belongs.

Related Commands	neighbor bfd — Explicitly enables a BFD session with a BGP neighbor or a BGP peer group.



Boot Command Line Interface

To access this BOOT_USER mode, first boot your Dell Networking platform. When you see the “Press ESC to stop auto-boot”, press the ESC key to log into BCLI

You enter BOOT_USER mode immediately, as indicated by the BOOT_USER# prompt.

 **NOTE: All commands in this chapter are in Boot_User mode. These commands are supported on the Dell Networking platform.**

You cannot use the Tab key to complete commands in this mode.

boot change

Change the primary, secondary, or default Dell Networking OS boot configuration.

Syntax	boot change <i>primary secondary default</i> }	
Parameters	<i>primary</i>	Enter the keyword primary to configure the boot parameters used in the first attempt to boot Dell Networking OS.
	<i>secondary</i>	Enter the keyword secondary to configure boot parameters used if the primary operating system boot selection is not available.
	<i>default</i>	Enter the keyword default to configure boot parameters used if the secondary operating system boot parameter selection is not available. You can configure this option to any of the available type, for example flash/usb/ftp/tftp.
Defaults	None	
Command Modes	BOOT_USER	
Command History	Version 9.0.2.0	Introduced on the S6000.
Usage Information	After entering the <code>boot change</code> command and selecting the parameters, press Enter . The software prompts you to enter the following:	
	• The boot device (flash, ftp, tftp, or usbflash), image file name, IP address of the server containing the image, username, and password (only for ftp).	
	Note When you enter a new parameter that extends beyond 80 characters, you cannot use the Backspace key to correct any mistakes. If you make a mistake, you must re-enter the parameter.	



Note: You must set the IP address of the designated download port before you execute this command. Otherwise, an second statement message alerts you that the configuration cannot proceed.

shows the first field after you enter **boot change primary**. At this point:

- Press **Enter** to accept the information already configured, or
- Change that information. To do so, press the . (period) key and enter new information. After you enter the information, press **Enter**.

Example

```
BOOT_USER # boot change primary
boot device : ftp
```

shows the completed command:

```
BOOT_USER # boot change primary
'.' = clear field; '-' = go to previous field
boot device : ftp
file name : tt/latestlabel
Server IP address : 10.16.1.200
username : amsterdam
password : *****
BOOT_USER #
```

To view the current boot configuration, use the **show bootvar** command.

Related Commands [boot_zero](#) — Remove the primary, secondary, or default boot image configuration.
 [show_bootvar](#) — Display boot configuration information.

boot message

Use this command to enable/disable boot logs during reload.

Syntax **boot message *on / off***

Parameters

<i>on</i>	Enter the keyword on to turn on boot logs during reload.
<i>off</i>	Enter the keyword off to suppress the boot logs during reload.



NOTE: By default, watchdog is disabled.

Defaults None

Command Modes BOOT_USER

Command History

Version 9.0.2.0	Introduced on the S6000.

Example

```
BOOT_USER #boot message
boot messages off
BOOT_USER #
```

boot show net config retries

Show the number of retries for network boot configuration failure.

Syntax	boot show net config retries	
Command Modes	BOOT_USER	
Command History	Version 9.0.2.0	Introduced on the S6000.
Example	<pre>BOOT_USER #boot show net config retries Number of Network Boot Config Retries is : 0 BOOT_USER #</pre>	

boot write net config retries

Set the number of retries for network boot configuration failure.

Syntax	boot write net config retries <int>	
Command Modes	BOOT_USER	
Command History	Version 9.0.2.0	Introduced on the S6000.
Example	<pre>BOOT_USER # boot write net config retries 2 Updated number of Network Boot Config retries to 2 BOOT_USER #</pre>	

boot zero

Erase the configured primary, secondary, or default boot image parameters. If you erase all three parameters, the S6000 switch boots from its internal Flash.

Syntax	boot zero <i>primary</i> <i>secondary</i> <i>default</i> }	
Parameters	<i>primary</i>	Enter the keyword primary to configure the boot parameters used in the first attempt to boot the system.
	<i>secondary</i>	Enter the keyword secondary to configure boot parameters used if the primary operating system boot selection is not available.



default

Enter the keyword **default** to configure boot parameters used if the secondary operating system boot parameter selection is not available. You can configure this option to any of the available type, for example flash/usb/ftp/tftp.

Defaults None

Command Modes BOOT_USER

Command History
Version 9.0.2.0 Introduced on the S6000.

Usage Information This command reverses changes made with the **boot change** command.

BOOT_USER # boot zero primary

BOOT_USER # boot zero secondary

BOOT_USER # boot zero default

BOOT_USER # show bootvar

PRIMARY OPERATING SYSTEM BOOT PARAMETERS:

=====

No Operating System boot parameters specified!

SECONDARY OPERATING SYSTEM BOOT PARAMETERS:

=====

No Operating System boot parameters specified!

DEFAULT OPERATING SYSTEM BOOT PARAMETERS:

=====

No Operating System boot parameters specified!

BOOT_USER #

Related Commands [boot change](#)— Change the primary, secondary, or default boot image configuration.

default-gateway

Assign an IP address as the default gateway for the system.

Syntax [no] **default-gateway** *ip-address*



Parameters	<i>ip-address</i>	Enter the IP address of the gateway router in dotted decimal format (A.B.C.D).
Command Modes	BOOT_USER	
Command History	Version 9.0.2.0	Introduced on the S6000.
Usage Information	Use the show default-gateway command to view the current default gateway.	
Related Commands	show-default-gateway — Change the primary, secondary, or default boot image configuration.	

etheraddr <macaddr>

Assign the management port MAC address.

Syntax	etheraddr <macaddr>	
Parameters	<i>mac-address</i>	Enter a MAC address in standard format.
Command Modes	BOOT_ADMIN	
Command History	Version 9.0.2.0	Introduced on the S6000.
Usage Information	Use this command to assign a MAC address if FTOS cannot find a default MAC address.	
Example	<pre>BOOT_ADMIN # etheraddr aa:aa:aa:aa:aa:aa <Macaddr> XX:xx:xx:xx:xx:xx No defaults for this</pre>	

ignore enable-password

Reload the system software without the enable password configured.

Syntax	ignore enable-password	
Command Modes	BOOT_USER	
Command History	Version 9.0.2.0	Introduced on the S6000.



Usage Information	When you enter the reload command and the system reboots, you will not be prompted for a password to enter the EXEC Privilege mode (normally you are required to enter the enable command). If your console or Telnet session expires after you used the ignore enable-password command, you are prompted for an enable password when you re-establish the session
Related Commands	reload — Exit from this mode and reload FTOS.

ignore startup-config

During a reload, do not load the startup-config file.

Syntax	ignore startup-config
Defaults	disabled
Command Modes	BOOT_USER
Command History	Version 9.0.2.0 Introduced on the S6000.
Usage Information	Use this command if you have authentication procedures in the startup-config other than the enable-password setting.

interface management ethernet ip address

Assign an IP address to the Management Ethernet interface.

Syntax	[no] interface management ethernet ip address <i>ip-address mask</i> To delete the IP address, enter no interface management ethernet ip address.
Defaults	Not configured.
Command Modes	BOOT_USER
Command History	Version 9.0.2.0 Introduced on the S6000.
Usage Information	In the runtime CLI, use the ip address command in INTERFACE mode to change the Management interface's IP address. To view the current IP address configured on the Management interface, enter the show interfaces management ethernet command
Related Commands	show default-gateway — Display the IP address configured for the default gateway.



[show_interface_mangement_ethernet](#)— Display the IP address configured for the Management interface.

NVRAM erase

Erase all NVRAM contents alone.

Syntax	nvramp erase	
Parameters	<i>mac-address</i>	Enter a MAC address in standard format.
Command Modes	BOOT_ADMIN	
Command History	Version 9.0.2.0	Introduced on the S6000.
Usage Information	Use this command to assign a MAC address if FTOS cannot find a default MAC address.	
Example	<pre>BOOT_USER # BOOT_ADMIN # nvramp erase Are you sure (y/n)? : yes Erasing NVRAM sectors....Erasing NvRam of size 1024 KB ... DONE</pre>	

reload

Exit from this mode and reload Dell Networking OS.

Syntax	reload	
Command Modes	BOOT_USER	
Command History	Version 9.0.2.0	Introduced on the S6000.

serial console

Use the serial console to set the serial console baud rate.

Syntax	serial console <int> <int>



Parameters	<i>serial console [unit] [baud]</i> Enter the keyword to set the serial port baud rate. The supported values for serial console: - Unit - 0 - Baud rate -9600,115200 No defaults.
Command Modes	BOOT_USER
Command History	Version 9.0.2.0 Introduced on the S6000.
Example Serial	<pre>BOOT_USER # serial console 0 9600 BOOT_USER # BOOT_USER #</pre>

show bootvar

Display boot configuration information.

Syntax	show bootvar
Command Modes	BOOT_USER
Command History	Version 9.0.2.0 Introduced on the S6000.
Example	<pre>BOOT_USER # show bootvar PRIMARY OPERATING SYSTEM BOOT PARAMETERS: ===== No Operating System boot parameters specified! SECONDARY OPERATING SYSTEM BOOT PARAMETERS: ===== boot device : flash file name : systema (FTOS system://A Partition) DEFAULT OPERATING SYSTEM BOOT PARAMETERS: ===== boot device : tftp</pre>



file name : PS-SI-9-0-0-566.bin

Management Ethernet IP address : 10.16.133.17

Mask : 255.255.0.0

Server IP address : 10.16.1.200

Default Gateway IP address : 10.16.1.254

BOOT_USER #

Related Commands [boot_change](#) — Change the primary, secondary, or default boot image configuration.
[boot_zero](#) — Erase the configured primary, secondary, or default boot image parameters.

show default-gateway

Display the IP address configured for the default gateway.

Syntax	show default-gateway
Command Modes	BOOT_USER
Command History	Version 9.0.2.0 Introduced on the S6000.
Example	<pre>BOOT_USER # show default-gateway Gateway IP address: 10.16.100.254 BOOT_USER #</pre>

Related Commands [default-gateway](#) — Configure the IP address for the default gateway.
[interface_management_ethernet_ip_address](#) — Assign an IP address to the Management Ethernet interface.

show interface management ethernet

Display the IP address configured for the Management interface.

Syntax	show interface management ethernet
Command Modes	BOOT_USER
Command History	Version 9.0.2.0 Introduced on the S6000.



Example	<pre> BOOT_USER # show interfaces management ethernet Management ethernet IP address: 10.16.133.17/24 BOOT_ADMIN # </pre> On the S6000, the output of this command includes the MAC address and port number of the assigned management port.
	<pre> BOOT_ADMIN # show int man eth Management ethernet IP address: 10.16.132.4/16 BOOT_ADMIN # </pre>
Related Commands	interface_management_ethernet_ip_address — Assign an IP address to the Management Ethernet interface.
	reload — Configure speed, duplex, and negotiation settings for the management interface.

show serial console baud rate

Use the show serial console to show the values of the serial console baud rate.

Syntax	show serial console baudrate
Command Modes	BOOT_USER
Command History	Version 9.0.2.0 Introduced on the S6000.
Example	<pre> BOOT_USER # show serial console baudrate Serial console baudrate = 9600 </pre>

watchdog <string>

Enable the watchdog timer, when the enabled watchdog timer is set to 60 seconds.

Syntax	<string> <i>enable disable status timeout settimeout</i> watchdog timer	
Parameters	<i>enable</i>	Enter the keyword enable to enable the watchdog.
	<i>disable</i>	Enter the keyword disable to disable the watchdog.
	<i>status</i>	Enter the keyword status to see the watchdog status.
	<i>timeout</i>	Enter the keyword timeout to see the timeout configured for the watchdog.



settimeout

Enter the keyword **set timeout** to set timeout.



NOTE: By default, watchdog is disabled.

Command Modes BOOT_ADMIN

Command History
Version 9.0.2.0 Introduced on the S6000.

Example

```
Boot_user#BOOT_ADMIN # watchdog status
```

```
WATCHDOG DISABLED
```

```
BOOT_ADMIN # watchdog enable
```

```
WATCHDOG ENABLED
```

```
BOOT_ADMIN # watchdog status
```

```
WATCHDOG ENABLED
```

```
BOOT_ADMIN # watchdog timeout
```

```
WATCHDOG TIMEOUT: 60
```



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.

BGP is supported in

 **NOTE:** For more information about configuring the border gateway protocol (BGP), refer to the BGP chapter in the *Dell Networking OS Configuration Guide*.

This chapter contains the following sections:

- BGPv4 Commands
- MBGP Commands
- BGP Extended Communities (RFC 4360)
- IPv6 BGP 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.

 **NOTE:** Dell Networking OS supports 2-byte (16-bit) and 4-byte (32-bit) format for autonomous system numbers (ASNs), where the 2-byte format is 1 to 65535 and the 4-byte format is 1 to 4294967295.

 **NOTE:** Dell Networking OS supports dotted format as well as the traditional plain format for AS numbers. The dot format is displayed when using the `show ip bgp` commands. To determine the comparable dot format for an ASN from a traditional format, use `ASN/65536`, `ASN%65536`. For more information about using the 2- or 4-byte format, refer to the *Dell Networking OS Configuration Guide*.

address-family

Enable the IPv4 multicast or the IPv6 address family.

Syntax `address-family [ipv4 {multicast | vrf vrf-name} | ipv6 unicast [vrf vrf-name]]`

Parameters

<code>ipv4 multicast</code>	Enter the keyword <code>ipv4</code> followed by the keyword <code>multicast</code> to enable BGPv4 multicast mode.
<code>ipv4 vrf vrf-name</code>	Enter the keyword <code>ipv4</code> followed by the keyword <code>vrf</code> and then the name of the VRF to enable VRF mode.



NOTE: Use this attribute to start a BGP instance corresponding to either a specific address family in a default VRF or an IPv4 address family in a non-default VRF.

ipv6 unicast

Enter the keyword `ipv6` followed by the keyword `unicast` to enable BGPv6 mode.

vrf vrf-name

(Optional) Enter the keyword `vrf` followed by the name of the VRF to install the IPv6 route in that VRF.



NOTE: It will not be possible to enable VRF mode for IPv6 unicast without configuring the corresponding IPv4 unicast mode for the same VRF. While deletion, whenever the IPv4 VRF mode is deleted for the VRF, it will automatically delete the IPv6 VRF configurations as well.

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
9.7(0.0)	Added support for IPv6 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.

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 <i>map-name</i>	(OPTIONAL) Enter the keywords <code>attribute-map</code> then the name of a configured route map to modify attributes of the aggregate, excluding <code>AS_PATH</code> and <code>NEXT_HOP</code> attributes.
summary-only	(OPTIONAL) Enter the keyword <code>summary-only</code> to advertise only the aggregate address. Specific routes are not advertised.
suppress-map <i>map-name</i>	(OPTIONAL) Enter the keywords <code>suppress-map</code> 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
9.7(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.

Syntax	bgp add-path [send receive both] <i>path-count</i>		
Parameters	send	Enter the keyword <code>send</code> to indicate that the system sends multiple paths to peers.	
	receive	Enter the keyword <code>receive</code> to indicate that the system accepts multiple paths from peers.	
	both	Enter the keyword <code>both</code> to indicate that the system sends and accepts multiple paths from peers.	
	<i>path-count</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .		

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.
9.0.2.0	Introduced on the S6000.
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.

Syntax	<code>bgp always-compare-med</code>
	To disable comparison of MED, enter <code>no bgp always-compare-med</code> .

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
9.7(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 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).

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
9.7(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.
8.3.1.0	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-octet-as-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.

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
9.7(0.0)	Introduced on the S6000–ON.
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.
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.

Syntax	<code>bgp bestpath as-path multipath-relax</code> To return to the default BGP routing process, use the <code>no bgp bestpath as-path multipath-relax</code> command.
Defaults	Disabled
Command Modes	ROUTER BGP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
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.

Syntax	<code>bgp bestpath med confed</code> To disable MED comparison on BGP confederation paths, enter the <code>no bgp bestpath med confed</code> 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
9.7(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 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.

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
9.7(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.
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.

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
9.7(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.
8.3.1.0	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.

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
9.7(0.0)	Introduced on the S6000–ON.
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.
7.8.1.0	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.

Syntax `bgp cluster-id {ip-address | number}`
To delete a cluster ID, use the `no bgp cluster-id {ip-address | number}` command.

Parameters

<i>ip-address</i>	Enter an IP address as the route reflector cluster ID.
<i>number</i>	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
9.7(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 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.

This command automatically restarts the BGP instance for the configuration to take effect.

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.

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
9.7(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. 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.

Dell Networking OS accepts confederation EBGP peers without a LOCAL_PREF attribute. The software sends AS_CONFED_SET and accepts AS_CONFED_SET and AS_CONF_SEQ.

If a local-as is configured, BGP does not allow for the configuration of BGP confederation. Similarly, if BGP confederation is configured, then BGP does not allow the configuration of local-as.

If the neighbor is an eBGP neighbor, then BGP performs a check on the first AS number. In this scenario, it is mandatory that the first sequence in the AS path is of type AS_SEQUENCE or AS_CONFED_SEQUENCE (in the case of confederations). If the first entry appears as an AS_CONFED_SET and the neighbor is not in the local AS, then this is strictly a problem with the neighbor node.

This command automatically restarts the BGP instance for the configuration to take effect.

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.

Syntax `bgp confederation peers as-number [...as-number]`
To return to the default, use the `no bgp confederation peers` command.

Parameters

<i>as-number</i>	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).
<i>...as-number</i>	(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
9.7(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.



Version	Description
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.
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.

Syntax	<pre>bgp dampening [<i>half-life reuse suppress max-suppress-time</i>] [route-map <i>map-name</i>]</pre> To disable route dampening, use the <code>no bgp dampening [<i>half-life reuse suppress max-suppress-time</i>] [route-map <i>map-name</i>]</code> command.

Parameters	<i>half-life</i> (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. <i>reuse</i> (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. <i>suppress</i> (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. <i>max-suppress-time</i> (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. <i>route-map map-name</i> (OPTIONAL) Enter the keyword <code>route-map</code> then the name of a configured route map. Only <code>match</code> 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
9.7(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

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.

Route refresh is sent when you enable BGP dampening.

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.

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
9.7(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.
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

Enables BGP Link Bandwidth.

Syntax `bgp dmzlink-bw`
To disable BGP Link Bandwidth, enter the `no bgp dmzlink-bw` command.

Parameters

dmzlink-bw	Enter the keyword <code>dmzlink-bw</code> 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.

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.

Syntax	<code>bgp enforce-first-as</code> To turn off the default, use the <code>no bgp enforce-first-as</code> command.
Defaults	Enabled
Command Modes	ROUTER BGP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
7.4.1.0	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 <code>show ip bgp neighbors</code> 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.

In the event of an enforce-first-as check failure, the existing BGP session is flapped.

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.

Syntax	<code>bgp fast-external-fallover</code>



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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 <code>bgp fast-external-fallover</code> command appears in the <code>show config</code> command output.

The fast external fallover configuration is applied only after you manually reset all the existing BGP sessions. As a result, after you execute this command, you must also manually execute the `clear ip bgp` command in order for the configuration to take effect.

bgp four-octet-as-support

Enable 4-byte support for the BGP process.

Syntax	<code>bgp four-octet-as-support</code> To disable fast external failover, use the <code>no bgp four-octet-as-support</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 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*.

This command automatically restarts the BGP instance for the configuration to take effect.

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.

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 <code>restart-time</code> 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 <code>stale-path-time</code> 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 <code>role receiver-only</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.
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.

This command automatically restarts the BGP instance for the configuration to take effect.

bgp non-deterministic-med

Compare MEDs of paths from different autonomous systems.

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
9.7(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 In Non-Deterministic mode, paths are compared in the order in which they arrive. This method can lead to Dell Networking OS 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`), Dell Networking OS 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 recursive-bgp-next-hop

Enable next-hop resolution through other routes learned by BGP.

Syntax	<code>bgp recursive-bgp-next-hop</code> To disable next-hop resolution, use the <code>no bgp recursive-bgp-next-hop</code> command.
Defaults	Enabled
Command Modes	ROUTER BGP
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 is a <i>knob</i> 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.

Syntax	<code>bgp regex-eval-optz-disable</code> To re-enable optimization engine, use the <code>no bgp regex-eval-optz-disable</code> 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
9.7(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

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.

Syntax	<code>bgp router-id ip-address</code> To delete a user-assigned IP address, use the <code>no bgp router-id</code> command.	
Parameters	<i>ip-address</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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	Peering sessions are reset when you change the router ID of a BGP router. This command automatically restarts the BGP instance for the configuration to take effect.

clear ip bgp

Reset BGP sessions. The soft parameter (BGP Soft Reconfiguration) clears the policies without resetting the TCP connection.

Syntax	<code>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]</code>	
Parameters	<i>vrf vrf-name</i>	Enter the keyword <code>vrf</code> 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 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 <code>soft</code> 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 <code>in</code> to activate only inbound policies.
out	(OPTIONAL) Enter the keyword <code>out</code> 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 <code>dampening</code> to clear the flap dampening information.
flap-statistics	Enter the keywords <code>flap-statistics</code> 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
9.0.2.0	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.
6.5.1.0	Expanded to include the <code>as-number</code> 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.

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
9.7(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 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.

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
9.7(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

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.

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
9.7(0.0)	Added the ipv4 multicast and ipv6 unicast parameters.
8.3.19.0	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.

debug ip bgp

Display all information on BGP, including BGP events, keepalives, notifications, and updates.

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 <code>vrf</code> 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 <code>peer-group</code> then the name of the peer group to debug.
in	(OPTIONAL) Enter the keyword <code>in</code> to view only information on inbound BGP routes.
out	(OPTIONAL) Enter the keyword <code>out</code> 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 <code>dampening</code> to view BGP dampening.
events	Enter the keyword <code>events</code> 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 <code>keepalives</code> to view BGP keepalives.
notifications	Enter the keyword <code>notifications</code> to view BGP notifications.
soft-reconfiguration	Enter the keywords <code>soft-reconfiguration</code> to view only information on inbound BGP soft reconfiguration.
updates	Enter the keyword <code>updates</code> 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.

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 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.

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 <code>vrf</code> followed by the name of the VRF to view information on dampened routes corresponding to that VRF.
	ipv4 multicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>multicast</code> to view dampened-route information related only to ipv4 multicast routes.
	ipv4 unicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>multicast</code> to view dampened-route information related only to ipv4 unicast routes.
	ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>unicast</code> 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
9.7(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.

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 <code>vrf</code> 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 <code>peer-group</code> then the name of the peer group.



in	(OPTIONAL) Enter the keyword <code>in</code> to view only events on inbound BGP messages.
out	(OPTIONAL) Enter the keyword <code>out</code> 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
9.7(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.

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 <code>vrf</code> 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 <code>peer-group</code> then the name of the peer group.
in	(OPTIONAL) Enter the keyword <code>in</code> to view only inbound keepalive messages.
out	(OPTIONAL) Enter the keyword <code>out</code> 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
9.7(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

Allows you to view information about BGP notifications received from neighbors.

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 <code>vrf</code> 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 <code>peer-group</code> then the name of the peer group.
in	(OPTIONAL) Enter the keyword <code>in</code> to view BGP notifications received from neighbors.
out	(OPTIONAL) Enter the keyword <code>out</code> 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
9.7(0.0)	Added ipv6 support.



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	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.

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
9.7(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.



Version	Description
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

Allows you to view information about BGP updates.

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 <code>vrf</code> 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 <code>peer-group</code> followed by the name of the peer group.
	in	(OPTIONAL) Enter the keyword <code>in</code> to view only BGP updates received from neighbors.
	out	(OPTIONAL) Enter the keyword <code>out</code> to view only BGP updates sent to neighbors.
	prefix-list prefix-list-name	(OPTIONAL) Enter the keyword <code>prefix-list</code> 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
9.7(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.



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 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.

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
9.7(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 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

Enables you to specify link band width 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
9.7(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

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
9.7(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.



Version	Description
pre-7.7.1.0	Introduced.

Related Commands [router bgp](#) — enters ROUTER mode on the switch.

maximum-paths

Configure the maximum number of parallel routes (multipath support) BGP supports.

Syntax `maximum-paths {ebgp | ibgp} number`
To return to the default values, enter the `no maximum-paths` command.

Parameters

ebgp	Enter the keyword <code>ebgp</code> to enable multipath support for External BGP routes.
ibgp	Enter the keyword <code>ibgp</code> to enable multipath support for Internal BGP routes.
number	Enter a number as the maximum number of parallel paths.

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
9.7(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 <code>max-path</code> (was <code>maximum-paths</code>).
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).

Syntax `neighbor [ip-address | peer-group-name] activate`



To disable, use the `no neighbor [ip-address | peer-group-name] activate` command.

Parameters	<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	(OPTIONAL) Enter the name of the peer group.
	<i>activate</i>	Enter the keyword <code>activate</code> 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
9.7(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 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.

It is not possible to de-activate a peer from the IPv4 unicast address family.

neighbor add-path

This command allows the specified neighbor/peer group to send/receive multiple path advertisements.

Syntax `neighbor [ip-address | peer-group-name] add-path [send | receive | both] path-count`

Parameters	<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	(OPTIONAL) Enter the name of the peer group.
	<i>send</i>	Enter the keyword <code>send</code> to indicate that the system sends multiple paths to peers.
	<i>receive</i>	Enter the keyword <code>receive</code> to indicate that the system accepts multiple paths from peers.
	<i>both</i>	Enter the keyword <code>both</code> 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
9.7(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	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.

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

<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
<i>seconds</i>	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
9.7(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.

neighbor advertisement-start

To send BGP routing updates, set the minimum interval before starting.

Syntax `neighbor {ip-address} advertisement-start seconds`
 To return to the default value, use the `no neighbor {ip-address} advertisement-start` command.

Parameters

<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
<i>seconds</i>	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
9.7(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.



neighbor allowas-in

Set the number of times an AS number can occur in the AS path.

Syntax	<code>neighbor {ip-address peer-group-name} allowas-in number</code> To return to the default value, use the <code>no neighbor {ip-address peer-group-name} allowas-in</code> command.															
Parameters	<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.														
	<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.														
	<i>number</i>	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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr></table>		Version	Description	9.7(0.0)	Introduced on the S6000–ON.	8.3.19.0	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															
9.7(0.0)	Introduced on the S6000–ON.															
8.3.19.0	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 cannot set this configuration for a peer that is associated with a peer group. Similarly, you cannot associate a peer to a peer group if that peer is already configured with these settings.															

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.

Syntax	<pre>neighbor {ip-address peer-group-name} default-originate [route-map map-name]</pre> To remove a default route, use the <code>no neighbor {ip-address peer-group-name} default-originate</code> command.



Parameters	<i>ip-address</i>	(OPTIONAL) Enter the IP address of the neighbor in dotted decimal format.
	<i>peer-group-name</i>	Enter the name of the peer group to set the default route of all routers in that peer group.
	<i>route-map map-name</i>	(OPTIONAL) Enter the keyword <code>route-map</code> 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
9.7(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 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.

When you configure a route-map for a BGP peer or peer group with the `neighbor default-originate` command, the command checks for the existence of the route in BGP RIB.

Route-map configuration on a BGP peer or peer group works only when the LOC-RIB contains at least one route.

When you apply a default route to a BGP peer or peer group using the `neighbor default-originate` command, changes to the configured default route-map are applied to the BGP peer or peer group only after a delay of 15 seconds. As a result, you must wait for a period of 15 seconds before manually resetting BGP using the `clear ip bgp` command.

In case of eBGP, the `neighbor default-originate` command does not support *extended-community* as a non-transitive route-map attribute.

You cannot set this configuration for a peer that is associated with a peer group. Similarly, you cannot associate a peer to a peer group if that peer is already configured with these settings.

In order that settings corresponding to the `neighbor default-originate` command take effect, you must execute the `clear ip bgp` command immediately after you execute the `neighbor default-originate` command.



neighbor description

Assign a character string describing the neighbor or group of neighbors (peer group).

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group.
<i>text</i>	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
9.7(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.

neighbor distribute-list

Distribute BGP information via an established prefix list.

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to apply the distribute list filter to all routers in the peer group.



<i>prefix-list-name</i>	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
9.7(0.0)	Introduced on the S6000–ON.
8.3.19.0	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 Other BGP filtering commands include: `neighbor filter-list`, `ip as-path access-list`, and `neighbor route-map`.

Related Commands [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.

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	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
9.7(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 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.

Syntax `neighbor {ipv4-address | peer-group-name} fall-over`
To disable, use the `no neighbor {ipv4-address | peer-group-name} fall-over` command.

Parameters

<i>ipv4-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	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
9.7(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.



Version	Description
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 local-as

To accept external routes from neighbors with a local AS number in the AS number path, configure Internal BGP (IBGP) routers.

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to set the advertisement interval for all routers in the peer group.
<i>as-number</i>	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).
<i>no prepend</i>	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
9.7(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 If a local-as is configured, BGP does not allow for the configuration of BGP confederation. Similarly, if BGP confederation is configured, then BGP does not allow the configuration of local-as.

This command automatically restarts the neighbor session for the configuration to take effect.

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.

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group.
<i>maximum</i>	Enter a number as the maximum number of prefixes allowed for this BGP router. The range is from 1 to 4294967295.
<i>threshold</i>	(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 .
<i>warning-only</i>	(OPTIONAL) Enter the keyword <code>warning-only</code> 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.



NOTE: When you set this option, the router accepts BGP prefixes only until the maximum configured value. After the maximum number is reached, the router drops any additional prefixes that it receives.

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
9.7(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.



Version	Description
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 password

Enable message digest 5 (MD5) authentication on the TCP connection between two neighbors.

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

<i>ip-address</i>	Enter the IP address of the router to be included in the peer group.
<i>peer-group-name</i>	Enter the name of a configured peer group.
<i>encryption-type</i>	(OPTIONAL) Enter 7 as the encryption type for the password entered. 7 means that the password is encrypted and hidden.
<i>password</i>	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
9.7(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.



Version	Description
7.7.1.0	Introduced on the C-Series.

Usage Information	This command automatically restarts the neighbor session for the configuration to take effect. 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 <code>peer-group-name</code> 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: <pre>%RPM0-P:RP1 %KERN-6-INT: No BGP MD5 from [peer's IP address] :179 to [local router's IP address]:65524</pre> Also, if you configure different passwords on the two routers, the following message appears on the console: <pre>%RPM0-P:RP1 %KERN-6-INT: BGP MD5 password mismatch from [peer's IP address] : 11502 to [local router's IP address] :179</pre>

neighbor peer-group (assigning peers)

Allows you to assign one peer to an existing peer group.

Syntax	<pre>neighbor {ip-address peer-group peer-group-name} dmzlink-bw</pre> To delete a peer from a peer group, use the <code>no neighbor {ip-address peer-group peer-group-name}</code> command. To disable dmzlink-dw for the peer group, use the <code>no neighbor ip-address dmzlink-dw</code> command.

Parameters	<table> <tr> <td><i>ip-address</i></td><td>Enter the IP address of the router to be included in the peer group.</td></tr> <tr> <td><i>peer-group-name</i></td><td>Enter the name of a configured peer group.</td></tr> <tr> <td><i>dmzlink-bw</i></td><td>Enter the keyword <code>dmzlink-bw</code> to attach a link bandwidth to received routes.</td></tr> </table>  NOTE: If <code>dmzlink-bw</code> is configured for a peer, in order for the BGP peer to advertise the prefixes with <code>dmzlink-bw</code> attached to it, you must reset the peer or peer-group using the <code>clear ip bgp session</code> command.	<i>ip-address</i>	Enter the IP address of the router to be included in the peer group.	<i>peer-group-name</i>	Enter the name of a configured peer group.	<i>dmzlink-bw</i>	Enter the keyword <code>dmzlink-bw</code> to attach a link bandwidth to received routes.
<i>ip-address</i>	Enter the IP address of the router to be included in the peer group.						
<i>peer-group-name</i>	Enter the name of a configured peer group.						
<i>dmzlink-bw</i>	Enter the keyword <code>dmzlink-bw</code> to attach a link bandwidth to received 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
9.7(0.0)	Added the dmzlink-bw parameter.
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

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 route-map](#)
- [neighbor route-reflector-client](#)

if a neighbor's configuration is more specific than its peer group's configuration, the neighbor may retain its configuration after it is added to the peer group. The neighbor's configuration does not affect outgoing updates.

A peer group must exist (be enabled) before you add a peer to it. If the peer group is disabled (shutdown), the peers within that group are also disabled (shutdown).

In BGP, you cannot associate a peer to a peer-group without configuring the remote-as for Internal BGP (IBGP) or External BGP (EBGP).

This command automatically restarts the neighbor session for the configuration to take effect.

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.

Syntax

`neighbor peer-group-name peer-group`



To delete a peer group, use the `no neighbor peer-group-name peer-group` command.

Parameters	<i>peer-group-name</i> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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	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.

Syntax	<code>neighbor peer-group-name peer-group passive [sessions]</code> To delete a passive peer-group, use the <code>no neighbor peer-group-name peer-group passive</code> command.
Parameters	<i>peer-group-name</i> 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 <i>Dell Networking OS Command Line Reference Guide</i> .



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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced the <code>limit</code> 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.

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

<i>ip-address</i>	Enter the IP address of the neighbor to enter the remote AS in its routing table.
<i>peer-group-name</i>	Enter the name of the peer group to enter the remote AS into routing tables of all routers within the peer group.
<i>number</i>	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
9.7(0.0)	Introduced on the S6000–ON.
8.3.19.0	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).

This command automatically restarts the neighbor session for the configuration to take effect.

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.

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

<i>ip-address</i>	Enter the IP address of the neighbor to remove the private AS numbers.
<i>peer-group-name</i>	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
9.7(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.
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.

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group.
<i>map-name</i>	Enter the name of an established route map.
	If the Route map is not configured, the default is deny (to drop all routes).
<i>in</i>	Enter the keyword <code>in</code> to filter inbound routes.
<i>out</i>	Enter the keyword <code>out</code> to filter outbound routes.



NOTE: This command sends routes to peers only if an outbound policy is configured and if there is a change in the existing outbound policy.

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
9.7(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.
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.

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	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
9.7(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.



Version	Description
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.

This command automatically restarts the neighbor session for the configuration to take effect.

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.

Syntax

```
neighbor {ip-address | peer-group-name} send-community [extended | standard]
```

To disable sending a COMMUNITY attribute, use the `no neighbor {ip-address | peer-group-name} send-community` command.

Parameters

<i>ip-address</i>	Enter the IP address of the peer router in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to send a COMMUNITY attribute to all routers within the peer group.
extended	(OPTIONAL) Enter the keyword <code>extended</code> to send extended community attribute.
standard	(OPTIONAL) Enter the keyword <code>standard</code> 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 9.0.2.0	Introduced on the S6000.
Version	Description
9.7(0.0)	Introduced on the S6000–ON.



Version	Description
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. In order that settings corresponding to the `neighbor send-community` command take effect, you must execute the `clear ip bgp` command immediately after you execute the `neighbor send-community` command.

If you do not set any of the optional parameters (standard or extended), then both standard as well as extended attributes are sent. If you set either the standard or extended parameter, only the attribute that is specified is sent.

neighbor shutdown

Disable a BGP neighbor or peer group.

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	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
9.7(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 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.

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

<i>ip-address</i>	Enter the IP address of the neighbor in dotted decimal format.
<i>peer-group-name</i>	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
9.7(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.
7.4.1.0	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.

You cannot set this configuration for a peer that is associated with a peer group. Similarly, you cannot associate a peer to a peer group if that peer is already configured with these settings.





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 timers

Set keepalive and hold time timers for a BGP neighbor or a peer group.

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

<i>ip-address</i>	Enter the IP address of the peer router in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to set the timers for all routers within the peer group.
<i>keepalive</i>	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 .
<i>holdtime</i>	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
9.7(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 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 update-source

Enable the E-Series software to use Loopback interfaces for TCP connections for BGP sessions.

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

<i>ip-address</i>	Enter the IP address of the peer router in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to disable all routers within the peer group.
<i>interface</i>	Enter the keyword <code>loopback</code> 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
9.7(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 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.

Neighbors are sorted according to the source and destination ip addresses. If an update-source ip address exists, then the source ip address determines the order in which the neighbors are displayed.

neighbor weight

Assign a weight to the neighbor connection, which is used to determine the best path.

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

<i>ip-address</i>	Enter the IP address of the peer router in dotted decimal format.
<i>peer-group-name</i>	Enter the name of the peer group to disable all routers within the peer group.
<i>weight</i>	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
9.7(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 In the Dell Networking OS best path selection process, the path with the highest weight value is preferred.

 **NOTE: In the Dell Networking OS 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.

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

<i>ip-address</i>	Enter an IP address in dotted decimal format of the network.
<i>mask</i>	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).
<i>route-map map-name</i>	(OPTIONAL) Enter the keyword <code>route-map</code> 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
9.7(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 inactive.

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.

Syntax `network ip-address mask backdoor`
To remove a network, use the `no network ip-address mask backdoor` command.

Parameters

<i>ip-address</i>	Enter an IP address in dotted decimal format of the network.
<i>mask</i>	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
9.7(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 Although Dell Networking OS 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

Enables you to specify link band width 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 <code>bandwidth</code> 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

Version	Description
9.7(0.0)	Introduced on the S-Series.

Related Commands [deny bandwidth](#) – link band width extended-community attribute as the matching criteria to deny incoming or outgoing traffic..

redistribute

Redistribute routes into BGP.

Syntax `redistribute {connected | static} [route-map map-name]`
To disable redistribution, use the `no redistribution {connected | static}` command.

Parameters

connected	Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.
static	Enter the keyword <code>static</code> to redistribute manually configured routes. These routes are treated as incomplete routes.
route-map <i>map-name</i>	(OPTIONAL) Enter the keyword <code>route-map</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 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 inactive.

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.

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	<i>process-id</i>	Enter the number of the OSPF process. The range is from 1 to 65535.
	<i>match external {1 2}</i>	(OPTIONAL) Enter the keywords <code>match external</code> to redistribute OSPF external routes. You can specify 1 or 2 to redistribute those routes only.
	<i>match internal</i>	(OPTIONAL) Enter the keywords <code>match internal</code> to redistribute OSPF internal routes only.
	<i>route-map map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> 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
9.7(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.
8.3.1.0	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, Dell Networking OS 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	<i>as-number</i> 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	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.	7.8.1.0	Introduced on the S-Series.	7.7.1.0	Introduced on the C-Series.
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.																
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 <code>router bgp</code> command to be accepted. If no interfaces are enabled for Layer 3, an error message appears: <pre>% Error: No router id configured</pre> BGP does not allow 23456 (AS-TRANS) as a configured AS number.																
Example	<pre>Dell(conf)#router bgp 3 Dell(conf-router_bgp)#</pre>																

set extcommunity bandwidth

Enables you to set extended community bandwidth.

Syntax	<pre>set extcommunity bandwidth</pre> To disable extended community bandwidth, enter the <code>no set extcommunity bandwidth</code> command.				
Parameters	<i>bandwidth</i> Enter the keyword <code>bandwidth</code> to enable extended community bandwidth. The range is from 0 to 102400.				
Defaults	N/A				
Command Modes	ROUTER MAP				
Command History	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S-Series.</td></tr> </table>	Version	Description	9.7(0.0)	Introduced on the S-Series.
Version	Description				
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.

show capture bgp-pdu neighbor

Display BGP packet capture information for an IPv4 address on the system.

Syntax `show capture bgp-pdu neighbor ipv4-address`

Parameters

<i>ipv4-address</i>	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
9.7(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.
7.5.1.0	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#

```

show config

View the current ROUTER BGP configuration.

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
9.7(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.

Example

```

Dell(conf-router_bgp)#show config
!
router bgp 100
 network 1.1.11.1/32
 network 1.1.12.1/32
 network 1.1.13.1/32
 neighbor 10.1.1.2 remote-as 200
 neighbor 10.1.1.2 no shutdown

```

show ip bgp

View the current BGP IPv4 routing table for the system.

Syntax `show ip bgp [vrf vrf-name] [ipv4 unicast] [network [network-mask] [longer-prefixes]]`



Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> and then the name of the VRF to view ipv4-unicast route information corresponding to that VRF.
ipv4 unicast	(OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 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 <code>longer-prefixes</code> to view all routes with a common prefix.

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
9.7(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 <code>add-path</code> option to the S4810. Output on the S4810 shows the <code>ADDPATH</code> 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.
Metric	Displays the BGP route's metric, if assigned.
LocPrf	Displays the BGP LOCAL_PREF attribute for the route.



Field	Description
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#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#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.

Syntax `show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] cluster-list [cluster-id]`

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> and then the name of the VRF to view cluster information of BGP neighbors corresponding to that VRF.
ipv4 multicast	(OPTIONAL) Enter the keywords <code>ipv4</code> followed by the keyword <code>multicast</code> to view information related only to ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>unicast</code> to view information related only to ipv4 unicast routes.



ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv6</code> followed by the keyword <code>unicast</code> to view information related to only 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
9.7(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
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.

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 <code>vrf</code> 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 <code>ipv4</code> followed by the keyword <code>unicast</code> to view information related only to ipv4 unicast routes.
ipv4 multicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>multicast</code> to view information related only to ipv4 multicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv6</code> followed by the keyword <code>unicast</code> 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 <code>local-as</code> 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 <code>no-advertise</code> 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` (0xFFFFF01) 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
9.7(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.
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.

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 <code>vrf</code> 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 <code>ipv4 unicast</code> to view information only related to ipv4 unicast routes.
ipv4 multicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>multicast</code> to view information related only to ipv4 multicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv6</code> followed by the keyword <code>unicast</code> 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
9.7(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 c11
Dell(config-community-list)#permit 1000:1
Dell(config-community-list)#end
Dell#show ip bgp community-list c11
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).

Syntax `show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] dampened-paths`

Parameters

vrf vrf-name	(OPTIONAL) Enter the keywords <code>vrf</code> and then the name of the VRF to view routes that are affected by a specific community list corresponding to that VRF.
ipv4 unicast	(OPTIONAL) Enter the keywords <code>ipv4</code> followed by the keyword <code>unicast</code> to view information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv6</code> followed by the keyword <code>unicast</code> 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
9.7(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.

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
9.7(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.



Version	Description
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 : NdRMPPrim 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 : NdPaTb1P 0x41a19088
NdASPTb1P 0x41a19090 : NdCommTb1P 0x41a19098 : NhOptTransTb1P 0x41a190a0 :
NdRRClsTb1P 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 : AlwaysCmpMed 0 : LocrHld 10 :
LocrRem 10 :
softReconfig 0x41a1a58c
DefMet 0 : AutoSumm 1 : NhopsP 0x41a0d100 : Starts 0 : Stops 0 : Opens 0
Closes 0 : Fails 0 : FataIs 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
BGRst 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 :
NdRTMAFTb1Ver 0 :
NdRibCtxAddr 1101110688
NdRibCtxAddrLen 255 : NdAFPrefix 0 : NdAfNLRIP 0 : NdAFNLRILen 0 :

```



```

NdAFWPttrP 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.

Syntax	show ip bgp [vrf <i>vrf-name</i>] [ipv4 { <i>multicast</i> <i>unicast</i> } ipv6 <i>unicast</i>] extcommunity-list [<i>list name</i>]	
Parameters	vrf <i>vrf-name</i>	(OPTIONAL) Enter the keywords <i>vrf</i> and then the name of the VRF to view information on all routes with extended community attributes corresponding to that VRF.
	ipv4 <i>multicast</i>	(OPTIONAL) Enter the keyword <i>ipv4</i> followed by the keyword <i>multicast</i> to view information related only to ipv4 multicast routes.
	ipv4 <i>unicast</i>	(OPTIONAL) Enter the keywords <i>ipv4 unicast</i> to view information only related to ipv4 unicast routes.
	ipv6 <i>unicast</i>	(OPTIONAL) Enter the keyword <i>ipv6</i> followed by the keyword <i>unicast</i> to view information related only to ipv6 unicast routes.
	<i>list name</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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

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.



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 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.

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 <code>vrf</code> 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 <code>ipv4</code> followed by the keyword <code>multicast</code> to view information related only to ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>unicast</code> to view information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv6</code> followed by the keyword <code>unicast</code> 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
9.7(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
400 500 600 i
*>  66.0.0.0/24      172.16.0.2
500 i

```

show ip bgp flap-statistics

View flap statistics on BGP routes.

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 <code>vrf</code> and then the name of the VRF to view flap statistics on BGP routes corresponding to that VRF.
ipv4 multicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>multicast</code> to view information related only to ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>unicast</code> to view information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv6</code> followed by the keyword <code>unicast</code> 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 <code>filter-list</code> 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
9.7(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 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.

Syntax `show ip bgp [vrf vrf-name] [ipv4 unicast] inconsistent-as`

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> and then the name of the VRF to view routes corresponding to the VRF that contain inconsistent originating AS numbers.
ipv4 unicast	(OPTIONAL) Enter the keywords <code>ipv4 unicast</code> to view information only related to ipv4 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
9.0.2.0	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 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--

Dell>sho ip bgp vrf testinconsistent-as
 BGP table version is 11, local router ID is 66.66.77.77
 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
*>n 11.11.11.11/32	0.0.0.0		0		32768 i
*>n 22.22.22.22/32	0.0.0.0		0		32768 i
I 32.32.32.32/32	60.0.0.2			100	0 400 500 i
I 32.32.33.33/32	60.0.0.2			100	0 400 500 i
*>n 33.33.33.33/32	0.0.0.0		0		32768 i
*>n 33.33.44.55/32	0.0.0.0		0		32768 i
*>n 44.44.44.44/32	0.0.0.0		0		32768 i
*>I 55.55.0.0/16	72.1.1.2			100	0 i
*>I 55.55.55.55/32	72.1.1.2		0	100	0 i
*>I 55.55.66.66/32	72.1.1.2		0	100	0 i
*>a 66.66.0.0/16	0.0.0.0				32768 i
*>n 66.66.66.77/32	0.0.0.0		0		32768 i
*>n 66.66.77.77/32	0.0.0.0		0		32768 i

show ip bgp neighbors

Allows you to view the information BGP neighbors exchange.

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.

<code>ipv4 multicast</code>	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>multicast</code> to view information related only to ipv4 multicast routes.
<code>ipv4 unicast</code>	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>unicast</code> to view information related only to ipv4 unicast routes.
<code>ipv6 unicast</code>	(OPTIONAL) Enter the keyword <code>ipv6</code> followed by the keyword <code>unicast</code> to view information related only to ipv6 unicast routes.
<code>ip-address</code>	(OPTIONAL) Enter the IP address of the neighbor to view only BGP information exchanged with that neighbor.
<code>advertised-routes</code>	(OPTIONAL) Enter the keywords <code>advertised-routes</code> to view only the routes the neighbor sent.
<code>dampened-routes</code>	(OPTIONAL) Enter the keywords <code>dampened-routes</code> to view information on dampened routes from the BGP neighbor.
<code>detail</code>	(OPTIONAL) Enter the keyword <code>detail</code> to view neighbor-specific internal information for the IPv4 Unicast address family.
<code>flap-statistics</code>	(OPTIONAL) Enter the keywords <code>flap-statistics</code> to view flap statistics on the neighbor's routes.
<code>routes</code>	(OPTIONAL) Enter the keyword <code>routes</code> to view only the neighbor's feasible routes.
<code>received-routes</code> <code>[network [network-mask]</code>	(OPTIONAL) Enter the keywords <code>received-routes</code> 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.

<code>denied-routes</code> <code>[network [network-mask]</code>	(OPTIONAL) Enter the keywords <code>denied-routes</code> 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
9.7(0.0)	Added the <code>ipv4 multicast</code> and <code>ipv6 unicast</code> 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
8.3.8.0	Added the <code>add-path</code> option to the S4810. Output on the S4810 shows the <code>ADDPATH</code> 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 <code>detail</code> option. Output now displays the default MED value.
7.2.1.0	Added the <code>received</code> and <code>denied route</code> options.
6.3.1.0	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: • 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.

The Lines Beginning with:	Description
(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.

Syntax `show ip bgp [vrf vrf-name] next-hop`

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
9.7(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.



Field	Description
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.

Syntax `show ip bgp[vrf vrf-name] paths [regex regular-expression]`

Parameters

vrf vrf-name (OPTIONAL) Enter the keyword `vrf` to view all path attributes in the BGP database corresponding to that VRF.



NOTE: Description You can use this attribute to view information on all path attributes in the BGP database that correspond to either a default or a non-default VRF.

regex 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
9.7(0.0)	Introduced on the S6000-ON.



Version	Description
9.4(0.0)	Added support for VRF for the S4810, S4820T, and S6000.
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 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 paths ?
community          Display community information
extcommunity        Display extended community information
regexp              Display path information based on a regular
expression
|                   Pipe through a command

Dell#show ip bgp paths
Total 2 Paths
Refcount Metric Path
1          0      200 i
1          0      200 i
```

show ip bgp paths community

View all unique COMMUNITY numbers in the BGP database.

Syntax `show ip bgp [vrf vrf-name] paths community`

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
9.7(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 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

Allows you to view information on the BGP peers in a peer group.

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 <code>detail</code> to view detailed status information of the peers in that peer group.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view status information of the peers in that peer group. The output is the same as that found in the <code>show ip bgp summary</code> 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
9.7(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 <code>add-path</code> option to the S4810. Output on the S4810 shows the <code>ADDPATH</code> 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 <code>*</code> 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.

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 Enter a regular expression then use one or a combination of the following
[character] 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
9.7(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

Allows you to view the status of all BGP connections.

Syntax

```
show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast]
summary
```



Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> 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 <code>ipv4</code> followed by the keyword <code>multicast</code> to view information related only to ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>unicast</code> to view information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv6</code> followed by the keyword <code>unicast</code> 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
9.7(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

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 thousand routes that contain exactly the same set of attributes, then the `cluster_id` count is 1. If these thousand 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 for thousand 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 will differ 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.



Field	Description
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 <code>show ip bgp community</code> 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	Display Example
Established	
< 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 <code>neighbor maximum-prefix</code> command, (prfxd) appears in this column. If the neighbor is not in Established stage, the current stage is displayed (Idle, Connect, Active, OpenSent, OpenConfirm). When the peer is transitioning



Field	Description
	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.

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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 E-Series.

Example

```
Dell#show running-config bgp
!
router bgp 100
```



```

network 1.1.11.1/32
network 1.1.12.1/32
network 1.1.13.1/32
neighbor 10.1.1.2 remote-as 200
neighbor 10.1.1.2 no shutdown
Dell#

```

timers bgp

Adjust the BGP Keep Alive and Hold Time timers.

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
9.7(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 on the E-Series.

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).

Dell Networking OS MBGP is implemented as per IETF RFC 1858.

BGPv4 is supported in the following:



debug ip bgp dampening

View information on routes being dampened.

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 <code>vrf</code> followed by the name of the VRF to view information on dampened routes corresponding to that VRF.
ipv4 multicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>multicast</code> to view dampened-route information related only to ipv4 multicast routes.
ipv4 unicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>multicast</code> to view dampened-route information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv4</code> followed by the keyword <code>unicast</code> 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
9.7(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

Define an administrative distance for routes.

Syntax `distance bgp external-distance internal-distance local-distance`
To return to default values, use the `no distance bgp` command.

Parameters

<i>external-distance</i>	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 .
<i>internal-distance</i>	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 .
<i>local-distance</i>	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
9.7(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.

show ip bgp dampened-paths

View BGP routes that are dampened (non-active).

Syntax `show ip bgp [vrf vrf-name] [ipv4 {multicast | unicast} | ipv6 unicast] dampened-paths`

Parameters

vrf vrf-name	(OPTIONAL) Enter the keywords <code>vrf</code> and then the name of the VRF to view routes that are affected by a specific community list corresponding to that VRF.
ipv4 unicast	(OPTIONAL) Enter the keywords <code>ipv4</code> followed by the keyword <code>unicast</code> to view information related only to ipv4 unicast routes.
ipv6 unicast	(OPTIONAL) Enter the keyword <code>ipv6</code> followed by the keyword <code>unicast</code> 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
9.7(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.



Field	Description
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#
```



Content Addressable Memory (CAM)

Content addressable memory (CAM) commands are supported on the Dell Networking platform.

 **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.

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

- Dell Networking OS supports CAM allocations on the C-Series and S-Series.
- 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]).
- Dell Networking OS 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).

Syntax

```
cam-acl {default | l2acl number ipv4acl number ipv6acl number ipv4qos
number l2qos number l2pt number ipmacacl number [vman-qos | vman-dual-qos
```



```
number] ecfmac1 number [nlbclusterac1 number] ipv4pbr number }openflow
number | fcoe number} [iscsiptac1 number] [vrfv4ac1 number]
```

Parameters

default	Use the default CAM profile settings and set the CAM as follows: • L2Acl : 6 • IPV4Acl : 4 • IPV6Acl : 0 • IPV4Qos : 2 • L2Qos : 1 • L2PT : 0 • IpMacAcl : 0 • VmanQos : 0 • VmanDualQos : 0 • EcfmAc1 : 0 • nlbclusterac1: 0 • FcoeAcl : 0 • iscsiOptAc1 : 0 • ipv4pbr : 0 • vrfv4Ac1 :0 • Openflow : 0 • fedgovacl : 0
l2acl number	Enter the keyword <code>l2ac1</code> and then the number of l2acl blocks. The range is from 1 to 8.
ipv4acl number	Enter the keyword <code>ipv4ac1</code> and then the number of FP blocks for IPv4. The range is from 0 to 8.
ipv6acl number	Enter the keyword <code>ipv6ac1</code> and then the number of FP blocks for IPv6. The range is from 0 to 4.
ipv4qos number	Enter the keyword <code>ipv4qos</code> and then the number of FP blocks for IPv4. The range is from 0 to 8.
l2qos number	Enter the keyword <code>l2qos</code> and then the number of FP blocks for l2 qos. The range is from 1to 8.
l2pt number	Enter the keyword <code>l2pt</code> and then the number of FP blocks for l2 protocol tunnelling. The range is from 0 to 1.
lpmacac1 number	Enter the keyword <code>lpmacac1</code> and then the number of FP blocks for IP and MAC ACL. The range is from 0 to 6.
ecfmac1 number	Enter the keyword <code>ecfmacac1</code> and then the number of FP blocks for ECFM ACL. The range is from 0 to 5.
nlbclusterac1 number	Enter the keyword <code>nlbclusterac1</code> 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.



NOTE: When you reconfigure CAM allocation, use the `nlbcluster acl number` command to change the number of NLB ARP entries. The range is from 0 to 2. The default value is 0. At the default value of 0, eight NLB ARP entries are available for use. This platform supports up to 512 CAM entries. Select 1 to configure 256 entries. Select 2 to configure 512 entries. Even though you can perform CAM carving to allocate the maximum number of NLB entries, Dell Networking recommends that you use a maximum of 64 NLB ARP entries.

<code>vman-qos vman-dual-qos number</code>	Enter the keyword <code>evman-qos</code> and then the number of FP blocks for VMAN QoS. The range is from 0 to 6.
<code>vman-dual-qos number</code>	Enter the keyword <code>vman-dual-qos</code> and then the number of FP blocks for VMAN dual QoS. The range is from 0 to 4.
<code>ipv4pbr number</code>	Enter the keyword <code>ipv4pbr</code> and then the number of FP blocks for ipv4pbr ACL. The range is from 0 to 8.
<code>Openflow number</code>	Enter the keyword <code>openflow</code> and then the number of FP blocks for open flow (multiples of 4). The range is from 0 to 8.
<code>fcoeacl number</code>	Enter the keyword <code>fcoeacl</code> and then the number of FP blocks for FCOE ACL. The range is from 0 to 6.
<code>iscsiptacl number</code>	Enter the keyword <code>iscsiptacl</code> and then the number of FP blocks for iSCSI optimization ACL. The range is from 0 to 2.
<code>l2acl number</code>	Allocate space to each CAM region.
<code>ipv4acl number</code>	Enter 4 or 8 for the number of OpenFlow FP blocks.
<code>ipv6acl number,</code>	
<code>ipv4qos number</code>	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)
<code>l2qos number 2pt number ipmacacl number ecfmact number</code>	
<code>{nlbclusteracl}</code>	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.
<code>[vman-qos vman-dual-qos number]</code>	
<code>ipv4pbr</code>	
<code>numberopenflow</code>	
<code>{4 8} fcoe number</code>	
<code>[iscsiptacl number]</code>	
<code>[vrfv4acl number]</code>	

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)	Added the <code>nlbcluster ACL</code> keyword. Introduced on the S6000-ON.
9.4.(0.0)	Added support for PBR and VRF.
9.2(0.2)	Added support for fcoe.



Version	Description
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 <code>ecfmac1</code> , <code>vman-qos</code> , and <code>vman-dual-qos</code> .
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 13 number of blocks can be configured by the user .

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.

Syntax `cam-acl-egress default | l2acl number ipv4acl number ipv6acl number`

Parameters

<i>default</i>	Reset egress CAM ACL entries to default settings.
<i>l2acl number</i>	Allocate space to each CAM region. The total space allocated must equal 4. The <code>ipv6acl</code> range must be a factor of 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
9.7(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.

cam-optimization

Optimize CAM utilization for QoS Entries by minimizing require policy-map CAM space.

Syntax	cam-optimization [qos]	
Parameters	qos	Optimize CAM usage for QoS.
Defaults	Disabled.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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 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).



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*.

show cam-acl

Display the details of the CAM profiles on the chassis and all stack units.

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
9.7(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 C-Series.

Usage Information

The display reflects the settings implemented with the `cam-acl` command.

Example

```
Dell#show cam-acl

-- Chassis Cam ACL --
                Current Settings(in block sizes)
                1 block = 256 entries
L2Acl           :      2
Ipv4Acl         :      4
Ipv6Acl         :      4
Ipv4Qos         :      2
L2Qos           :      1
L2PT            :      0
IpMacAcl        :      0
VmanQos         :      0
EcfmAcl         :      0
FcoeAcl         :      0
iscsiOptAcl     :      0
ipv4pbr         :      0
vrfv4Acl        :      0
Openflow        :      0
fedgovacl       :      0
nlbclusteracl   :      0

-- stack-unit 1 --
                Current Settings(in block sizes)
                1 block = 256 entries
L2Acl           :      2
Ipv4Acl         :      4
Ipv6Acl         :      4
Ipv4Qos         :      2
L2Qos           :      1
L2PT            :      0
IpMacAcl        :      0
VmanQos         :      0
EcfmAcl         :      0
FcoeAcl         :      0
iscsiOptAcl     :      0
ipv4pbr         :      0
vrfv4Acl        :      0
Openflow        :      0
fedgovacl       :      0
nlbclusteracl   :      0

-- stack-unit 3 --
                Current Settings(in block sizes)
                1 block = 256 entries
L2Acl           :      2
```



```

Ipv4Acl      :      4
Ipv6Acl      :      4
Ipv4Qos      :      2
L2Qos        :      1
L2PT         :      0
IpMacAcl     :      0
VmanQos      :      0
EcfmAcl      :      0
FcoeAcl      :      0
iscsiOptAcl  :      0
ipv4pbr      :      0
vrfv4Acl     :      0
Openflow     :      0
fedgovacl    :      0
nlbclusteracl :      0

```

test cam-usage

Verify that enough CAM space is available for the IPv6 ACLs you have created.

Syntax `test cam-usage service-policy input input policy name stack-unit {number | all}`

Parameters

<i>policy-map name</i>	Enter the name of the policy-map to verify. Maximum is 32 characters.
<i>number</i>	Enter <i>all</i> to get information for all the linecards/stack-units or enter the linecard/ stack-unit number to get information for a specific card. The range is 0-7 for all other S-Series. The range is 1-6.

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
97(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.

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
Stack-Unit	Lists the stack unit or units that are checked. Entering all shows the status for all stacks.
Portpipe	Lists the portpipe (port-set) or port pipes (port-sets) that are checked. Entering all shows the status for linecards or stack units and port-pipes in the chassis. The port set value is from 0 to 0.
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 (S-Series)

```

Dell#test cam-usage service-policy input In stack-unit all
Stack-Unit | Portpipe | CAM Partition | Available CAM | Estimated CAM per Port| Stat
-----
1 | 0 | IPv4Flow | 102 | 0| Allowed
1 | 0 | IPv4Flow | 102 | 0| Allowed
Dell#
!
Dell#test cam-usage service-policy input In stack-unit 1 port-set 0
Stack-Unit | Portpipe | CAM Partition | Available CAM | Estimated CAM per Port| Stat
-----
1 | 0 | IPv4Flow | 102 | 0| Allowed
Dell#

```

Usage Information

The following describes the test cam-usage command shown in the Example below.

Term	Explanation
Stack-Unit	Lists the stack unit or units that are checked. Entering all shows the status for all stacks.
Portpipe	Lists the portpipe (port-set) or port pipes (port-sets) that are checked. Entering all shows the status for linecards and port-pipes in the chassis.
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 (S-Series)

```

Dell#test cam-usage service-policy input LauraIn stack-unit all
Stack-Unit|Portpipe|CAM Partition|AvailableCAM|EstimatedCAM per Port|Status
-----
          1|          0|    IPv4Flow|          102|          0|Allowed
          1|          0|    IPv4Flow|          102|          0|Allowed
Dell#
!
Dell#test cam-usage service-policy input LauraIn stack-unit 0 port-set 0
Stack-Unit|Portpipe|CAM Partition|Available CAM|EstimatedCAM per Port|Status
-----
          1|          0|    IPv4Flow|          102|          0|Allowed
Dell#

```



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-I3–hosts (UFT mode 3) and scaled-I3–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.

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	<code>hardware forwarding-table mode {scaled-I3- hosts scaled-I3-routes}</code>	
Parameters	scaled-I3-hosts	Enter the keyword <code>scaled-I3-hosts</code> to select the forwarding table mode for scaling I3 host entries..
	scaled-I3-routes	Enter the keyword <code>scaled-I3-routes</code> to select the forwarding table mode for scaling I3 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 <i>Dell Networking OS Command Line Reference Guide</i> .	
	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, S6000-ON, and Z9500 switch..
Usage Information	This command takes effect only after reboot.	
Related Commands	show hardware forwarding-table mode — displays the hardware forwarding table mode in the current boot and in the next boot.	

show hardware forwarding-table mode

Display the hardware forwarding table mode in the current boot and in the next boot.

Syntax	<code>show hardware forwarding-table mode</code>
Defaults	none
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .
	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, S6000-ON, and Z9500 switch.

Example

```
Dell#show hardware forwarding-table mode

Mode                : Current Settings      Next Boot Settings
L2 MAC Entries      : 160K                  scaled-l3-hosts
L3 Host Entries      : 144K                  96K
L3 Route Entries     : 16K                   208K
                    :                       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.



Control Plane Policing (CoPP)

The CoPP commands are supported on the Dell Networking platform.

control-plane-cpuqos

To manage control-plane traffic, enter control-plane mode and configure the switch.

Syntax	<code>control-plane-cpuqos</code>
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

service-policy rate-limit-cpu-queues

Apply a policy map for the system to rate limit control traffic on a per-queue basis.

Syntax	<code>service-policy rate-limit-cpu-queues <i>policy-name</i></code>
Parameters	<i>policy-name</i> 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, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	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.

For CoPP, use the keyword `cpu-qos` when creating qos-policy-input.

Related Commands [qos-policy-input](#) — creates a QoS input policy map.

[policy-map-input](#) — creates an input policy map.

service-policy rate-limit-protocols

Apply a policy for the system to rate limit control protocols on a per-protocol basis.

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, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.



Version	Description
8.3.8.0	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.

For CoPP, use the keyword `cpu-qos` when creating qos-policy-input.

Related Commands [ip access-list extended](#) — creates an extended IP ACL.

[mac access-list extended](#) — creates an extended MAC ACL.

[qos-policy-input](#) — creates a QoS input policy map.

[class-map](#) — creates a QoS class map.

[policy-map-input](#) — creates an input policy map.

show cpu-queue rate cp

Display the rates for each CPU queue.

Syntax `show cpu-queue rate cp`

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
9.7(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	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.

Example

```
Dell#show cpu-queue rate cp
Service-Queue      Rate (PPS)      Burst ()
```



Q0	1300	512
Q1	300	50
Q2	300	50
Q3	400	50
Q4	2000	50
Q5	300	50
Q6	400	50
Q7	400	50
Q8	400	50
Q9	600	50
Q10	300	50
Q11	300	50

show ip protocol-queue-mapping

Display the queue mapping for each configured protocol.

Syntax `show ip 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
9.7(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	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   -         Q9     -        -
UDP (DHCP)  67/68     68/67     -         Q10    -        -
UDP (DHCP-R) 67        67        -         Q10    -        -
TCP (FTP)   any       21        -         Q6     -        -
ICMP        any       any       -         Q6     -        -
IGMP        any       any       -         Q11    -        -
TCP (MSDP)  any/639   639/any   -         Q11    -        -
UDP (NTP)   any       123       -         Q6     -        -
OSPF        any       any       -         Q9     -        -
PIM         any       any       -         Q11    -        -
UDP (RIP)   any       520       -         Q9     -        -
TCP (SSH)   any       22        -         Q6     -        -
TCP (TELNET) any       23        -         Q6     -        -
VRRP        any       any       -         Q10    -        -
Dell#
Dell#
```

Dell#
Dell#
Dell#

show ipv6 protocol-queue-mapping

Display the queue mapping for each configured IPv6 protocol.

Syntax `show ipv6 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
9.7(0.0)	Introduced on the S6000-ON.
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 ipv6 protocol-queue-mapping
  Protocol  Src-Port  Dst-Port  TcpFlag  Queue  EgPort  Rate (kbps)
  -----  -
TCP (BGP)   any/179   179/any   -         Q9     -        -
ICMPV6 NA   any       any       -         Q6     -        -
ICMPV6 RA   any       any       -         Q6     -        -
ICMPV6 NS   any       any       -         Q5     -        -
ICMPV6 RS   any       any       -         Q5     -        -
ICMPV6      any       any       -         Q6     -        -
VRRPV6     any       any       -         Q10    -        -
OSPFV3     any       any       -         Q9     -        -
Dell#
Dell#
Dell#
```

show mac protocol-queue-mapping

Display the queue mapping for the MAC protocols.

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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.8.0	Introduced on the S4810.

Example

```

Dell#show mac protocol-queue-mapping
  Protocol      Destination Mac      EtherType      Queue      EgPort
  Rate (kbps)
  -----
  -----
  ARP           any                  0x0806         Q5/Q6
  CP
  FRRP          01:01:e8:00:00:10/11 any             Q7
  CP
  LACP          01:80:c2:00:00:02    0x8809         Q7
  CP
  LLDP          any                  0x88cc         Q8
  CP
  GVRP          01:80:c2:00:00:21    any             Q8
  CP
  STP           01:80:c2:00:00:00    any             Q7
  CP
  ISIS          01:80:c2:00:00:14/15 any             Q9
  CP
  CP           09:00:2b:00:00:04/05 any             Q9
  CP
Dell#

```



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](#)

DCB Command

The following DCB command is supported on the Dell Networking OS.

dcb-enable

Enable data center bridging.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.3.16.0	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.

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 pfc counters

Clear the PFC TLV counters and PFC statistics on an interface or stack unit.

Syntax `clear pfc counters [port-type slot/port[/subport] | stack-unit {unit number | all } all stack-ports all}}`

Parameters	port-type	Enter the keywords <code>port-type</code> then the slot/port[/subport] information. Enter the subport number if a 40G port is fanned-out into 10G ports.
	stack-unit unit number	Enter the keywords <code>stack-unit</code> then the stack-unit number to be cleared.
	all stack-ports all	Enter the keywords <code>all stack-ports all</code> to clear the counters on all interfaces.
	statistics	Enter the keyword <code>statistics</code> 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
9.7(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.



pfc no-drop queues

Configure the port queues that still function as no-drop queues for lossless traffic.

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.

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
9.7(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 priority

Configure the CoS traffic to be stopped for the specified delay.

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 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on the S4810.
Version 8.3.16.0	Introduced on the MXL 10/40GbE Switch IO Module.

Usage Information



NOTE: Please note that Dell Networking does not recommended 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

Displays the data center bridging status, the number of PFC-enabled ports, and the number of PFC-enabled queues.

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
9.7(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 interface pfc

Displays the PFC configuration applied to ingress traffic on an interface, including priorities and link delay.

Syntax `show interface port-type slot/port[/subport] pfc {summary | detail}`

Parameters

port-type slot/ port[/subport] pfc	Enter the port-type slot and port PFC information. Enter the subport number if a 40G port is fanned-out into 10G ports.
{summary detail}	Enter the keyword <code>summary</code> for a summary list of results or enter the keyword <code>detail</code> for a full list of results.

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
9.2.(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[/subport]` command.

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.



Field	Description
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: • <code>Init</code>: Local PFC configuration parameters were exchanged with the peer. • <code>Recommend</code>: Remote PFC configuration parameters were received from the peer. • <code>Internally propagated</code>: 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.
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.



Field	Description
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 1/4/2 pfc summary
Interface TenGigabitEthernet 1/4/2
  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 1/4/2 pfc detail
Interface TenGigabitEthernet 1/4/2
  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

```

show interface pfc statistics

Displays counters for the PFC frames received and transmitted (by dot1p priority class) on an interface.

Syntax `show interface port-type slot/port[/subport] pfc statistics`



Parameters

<i>port-type</i>	Enter the port type.
<i>slot/port [/subport]</i>	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, refer to the relevant *Dell 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.
9.0.2.0	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.

Example (Summary)

```
Dell#show int te 1/1/1 pfc statistics
Interface TenGigabitEthernet 1/1/1
Priority      Rx XOFF Frames      Rx Total Frames      Tx
-----
-
0             0             0
1             0             0
2             0             0
3             0             0
4             0             0
5             0             0
6             0             0
0
7             0             0
```

ETS Commands

The following ETS commands are supported on the Dell Networking OS.

dcb-enable

Enable data center bridging.

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
9.7(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.

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.

clear ets counters

Clear all ETS TLV counters on an interface.

Syntax `clear ets counters port-type slot/port[/subport]`

Parameters

port-type	Enter the keywords <code>port-type</code> then the slot/port information. Enter the subport number if a 40G port is fanned-out into 10G ports.

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
9.7(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 interface ets

Displays the ETS configuration applied to egress traffic on an interface, including priority groups with priorities and bandwidth allocation.

Syntax `show interface port-type slot/port[/subport] ets {summary | detail}`

Parameters

<code>port-type slot/port[/subport] ets</code>	Enter the port-type slot and port ETS information. Enter the subport number if a 40G port is fanned-out into 10G ports.
<code>{summary detail}</code>	Enter the keyword <code>summary</code> for a summary list of results or enter the keyword <code>detail</code> for a full list of results.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
9.2(0.2)	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.

Example (Summary) `Dell#show interface te 1/3/1 ets de`

```
Interface TenGigabitEthernet 1/3/1
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		-	-

```

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# show int te 1/3/1 ets de
```

```

Interface TenGigabitEthernet 1/3/1
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		-	-

```

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		-	-

```

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# show interfaces tengigabitethernet 1/1/1 ets detail
Interface TenGigabitEthernet 1/1/1
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 1/1/1 ets detail
Interface TenGigabitEthernet 1/1/1
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

```

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.

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, refer to the relevant *Dell 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.
9.0.2.0	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.

dcbx port-role

Configure the DCBX port role the interface uses to exchange DCB information.

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 from 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, refer to the relevant *Dell 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.
9.0.2.0	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.

dcbx version

Configure the DCBX version used on the interface.

Syntax

`dcbx version {auto | cee | cin | ieee-v2.5}`

To remove the DCBX version, use the `dcbx version {auto | cee | cin | ieee-v2.5}` 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 <code>show interface dcbx detail</code> command.

debug dcbx

Enable DCBX debugging.

Syntax	<code>debug dcbx {all auto-detect-timer config-exchng fail mgmt resource sem tlv}</code>
	To disable DCBX debugging, use the <code>no debug dcbx</code> 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

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, refer to the relevant *Dell 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.
9.0.2.0	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.

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, refer to the relevant *Dell 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.
9.0.2.0	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

Displays the DCBX configuration on an interface.

Syntax `show interface port-type slot/port[/subport] dcbx detail`

Parameters

<i>port-type</i>	Enter the port type.
<i>slot/port</i> [/ <i>subport</i>]	Enter the slot/port number. Enter the subport number if a 40G port is fanned-out into 10G ports.

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
9.7(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.

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.



Field	Description
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.
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.



Field	Description
Total DCBX Frame errors	Number of DCBX frames with errors received.
Total DCBX Frames unrecognized	Number of unrecognizable DCBX frames received.

Example

```
Dell#show interface tengigabitethernet 1/9/1 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 1/9/1
  Remote Mac Address 00:00:00:00:00:11
  Port Role is Auto-Upstream
  DCBX Operational Status is Enabled
  Is Configuration Source? TRUE

Local DCBX Compatibility mode is CEE
  Local DCBX Configured mode is CEE
  Peer Operating version is CEE
  Local DCBX TLVs Transmitted: ErPfi

Local DCBX Status
-----
  DCBX Operational Version is 0
  DCBX Max Version Supported is 0
  Sequence Number: 2
  Acknowledgment Number: 2
  Protocol State: In-Sync

Peer DCBX Status:
-----
  DCBX Operational Version is 0
  DCBX Max Version Supported is 255
  Sequence Number: 2
  Acknowledgment Number: 2
  Total DCBX Frames transmitted 27
  Total DCBX Frames received 6
  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.

Syntax

```
dcb-map map-name
```



Parameters	<i>map-name</i>	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	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.3(0.0)</td><td>Introduced on the S4810 and S6000 platforms.</td></tr></table>	Version	Description	9.7(0.0)	Introduced on the S6000-ON.	9.3(0.0)	Introduced on the S4810 and S6000 platforms.	
Version	Description							
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 <code>show qos dcb-map</code> command. Use the <code>dcb-map</code> 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 <code>dcb-map</code> command is supported only on physical Ethernet interfaces. To remove a DCB map from an interface, enter the <code>no dcb-map map-name</code> command in Interface configuration mode.							

priority-pgid

Assign 802.1p priority traffic to a priority group in a DCB map.

Syntax	<pre>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</pre>	
Parameters	<i>dot1p0_group-num</i> <i>dot1p1_group-num</i> <i>dot1p2_group-num</i> <i>dot1p3_group-num</i> <i>dot1p4_group-num</i> <i>dot1p5_group-num</i> <i>dot1p6_group-num</i> <i>dot1p7_group-num</i>	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
	9.7(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 <code>dcb-map</code> command to configure different groups of 802.1p priorities with PFC and ETS settings. Using the <code>priority-pgid</code> 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 <code>priority-pgid 0 0 0 1 2 4 4 4</code> 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 <code>no priority-pgid</code> command.	

priority-group bandwidth pfc

Configure the ETS bandwidth allocation and PFC mode used to manage port traffic in an 802.1p priority group.

Parameters	priority-group group-num	Enter the keyword <code>priority-group</code> followed by the number of an 802.1p priority group. Use the <code>priority-pgid</code> command to create the priority groups in a DCB map.
	bandwidth percentage	Enter the keyword <code>bandwidth</code> 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
	9.7(0.0)	Introduced on the S6000-ON.



Version	Description
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.

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
9.7(0.0)	Introduced on the S6000-ON.



Version	Description
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 validation is performed to determine whether following condition is satisfied: $\text{Shared-pfc-buffer-size} \leq (\text{Total-pfc-buffer-size} - \sum \text{pfc priority} \times \text{buffer-size on each port, priority})$.

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.

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
9.7(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:

$\text{Shared-pfc-buffer-size} \leq (\text{Total-pfc-buffer-size} - \sum \text{pfc priority} \times \text{buffer-size on each port, priority})$.

```
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. This utility is supported on the S4810, S4820T, and S6000 platforms.

Syntax	<code>dcb buffer-threshold <i>profile-name</i></code>	
Parameters	<i>profile-name</i>	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
	9.7(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.	
Example	<code>S4810-YU-MR-Dell (conf) #dcb buffer-threshold test</code>	

priority

Configure the priority for the PFC threshold to be allocated to the buffer space parameters. This utility is supported on the platforms.

Syntax	<code>priority <i>value</i> buffer-size <i>size</i> pause-threshold <i>threshold-value</i> resume-offset <i>threshold-value</i> shared-threshold-weight <i>size</i></code>	
Parameters	<i>priority</i>	Specify the priority of the queue for which the buffer space settings apply
	<i>value</i>	Enter a number in the range of 0 to 7 to denote the priority to be allocated to the dynamic buffer control mechanism
	<i>buffer-size</i>	Ingress buffer size
	<i>size</i>	Size of the ingress buffer in KB. Enter a number in the range of 0 to 7787. The default is 45 KB.
	<i>pause-threshold</i>	Buffer limit for pause frames to be sent
	<i>threshold-value</i>	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.
	<i>resume-offset</i>	Buffer offset limit for resuming in KB
	<i>threshold-value</i>	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.
	<i>shared-threshold-weight</i>	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
	9.7(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 <code>priority</code> 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	<pre>Dell(conf-dcb-buffer-thr)#priority 0 buffer-size 52 pause-threshold 16 resume-offset 10 shared-threshold-weight 7</pre>	

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. This utility is supported on the platform.

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
9.7(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.

Syntax	<code>dcb-policy buffer-threshold <i>profile-name</i></code>	
Parameters	buffer-threshold	Configure the profile name for the DCB buffer threshold
	<i>profile-name</i>	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	Version	Description
	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.	
Example	<code>Dell(conf-if-te-1/1/1)#dcb-policy buffer-threshold test</code>	

show qos dcb-buffer-threshold

Displays the DCB buffer threshold assigned to a QoS policy. This command is supported on the platform.

Syntax	<code>show qos dcb buffer-threshold {<i>name</i>}</code>	
Parameters	<i>name</i>	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
	9.7(0.0)	Introduced on the S6000-ON.



Version	Description
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
```

dcb pfc-total-buffer-size

Configure the total buffer size for PFC in kilobytes. This utility is supported on the S6000 platform.

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
	9.7(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

Displays the DCB buffer threshold details in the running configuration.

Syntax `show running-config buffer-threshold`

Command Modes EXEC

EXEC Privilege

Command History

Version	Description
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 is applied
buffer-size	Ingress buffer size
pause-threshold-value	Buffer limit at which the port sends the pause to peer
resume-threshold-value	Buffer offset limit at which the port resumes the peer

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 1/1/1 pfc buffer-threshold
```

Queue#	Lossless	Buffer-size (KB)	Pause-threshold (KB)	Resume-offset (KB)	Shared weight
0	No	-	-	-	
1	No	-	-	-	
2	Yes	-	20	-	
3	Yes	52	25	15	
4	Yes	-	45	25	



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 1/20/1 pfc buffer-threshold
```

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 the threshold is configured
buffer-size	Ingress buffer size
pause-threshold-value	Buffer limit at which the port sends the pause to peer
resume-threshold-value	Buffer offset limit at which the port resumes the peer
shared threshold weight	Weightage of the priorities on the shared buffer size in the system.

dcb pfc-queues

Configure the number of PFC queues. This utility is supported on the S4810 and S6000 platforms.

Syntax	<code>dcb pfc-queues value</code>	
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 mode	
Command History	Version	Description
	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	<code>Dell(conf)#dcb pfc-queues 4</code>	



dcb {ets | pfc} enable

Enable priority flow control or enhanced transmission selection on interface.

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
9.7(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.



Debugging and Diagnostics

The basic debugging and diagnostic commands are supported by the Dell Networking Operating System.

This chapter contains the following sections:

- Diagnostic and Monitoring Commands
- Offline Diagnostic Commands
- Hardware Commands

Diagnostics and Monitoring Commands

The following section describes the diagnostics and monitoring commands.

For similar commands, refer to the [Control and Monitoring](#) chapter.

logging coredump stack-unit

Enable coredump on a stack.

Syntax `logging coredump stack-unit {stack-unit-number | all}`

Parameters

<i>stack-unit stack-unit-number</i>	Enter the stack-unit id. The range is from 1 to 6.
all	Enable coredump on all stack-unit.

Defaults Enabled by default on customer builds.

Command Modes CONFIGURATION

Command History

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.

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.



Offline Diagnostic Commands

The offline diagnostics test suite is useful for isolating faults and debugging hardware. While tests are running, Dell Networking OS results are saved as a text file (TestReport-SU-X.txt) in the flash directory. This `show file` command is available only on master and standby.

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.
- Diagnostics only test connectivity, not the entire data path.

diag stack-unit

Run offline diagnostics on a stack unit.

Syntax	<code>diag stack-unit <i>number</i> [alllevels level0 level1 level2] verbose testname</code>	
Parameters	<i>number</i>	Enter the stack-unit id. The range is from 1 to 6.
	alllevels	Enter the keyword <code>alllevels</code> to run the complete set of offline diagnostic tests.
	level0	Enter the keyword <code>level0</code> 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 <code>level1</code> 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, stack ports are shut down automatically.
	level2	Enter the keyword <code>level2</code> 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. To test 10G links, physically remove the unit from the stack.
	verbose	Enter the keyword <code>verbose</code> to run the diagnostic in Verbose mode. Verbose mode gives more information in the output than Standard mode.
	testname	Enter the keyword <code>testname</code> to run a specific test case. Enclose the test case name in double quotes (" "). For example: <code>diag stack-unit 1 level1 testname "first"</code> . You can use this option only for interactive tests.
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
9.7(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.
8.3.1.0	Introduced the <code>verbose</code> option.
7.7.1.0	Introduced on the S-Series.

offline stack-unit

Place a stack unit in the offline state.

Syntax `offline stack-unit number`

Parameters

<i>number</i>	Enter the stack-unit id.
	The range is from 1 to 6.

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
9.7(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	Added a warning message to the off-line diagnostic.
7.7.1.0	Introduced on the S-Series.

Usage Information You cannot enter this command on a Master or Standby unit.

The system reboots when the off-line diagnostics complete. This reboot is an automatic process. A warning message appears when the `offline stack-unit` command is implemented.



Warning - Diagnostic execution will cause stack-unit to reboot after completion of diags.

Proceed with Offline-Diags [confirm yes/no]:y

online stack-unit

Place a stack unit in the online state.

Syntax `online stack-unit number`

Parameters *number* Enter the stack-unit number. The range is from 1 to 6.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4810.
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.

Usage Information You cannot enter this command on a Master or Standby unit.

The system reboots when the off-line diagnostics complete. This reboot is an automatic process. A warning message appears when the `offline stack-unit` command is implemented.

Warning - Diagnostic execution will cause stack-unit to reboot after completion of diags.

Proceed with Offline-Diags [confirm yes/no]:y



Hardware Commands

These commands display information from a hardware sub-component or ASIC.

clear hardware stack-unit

Clear statistics from selected hardware components.

Syntax `clear hardware stack-unit id {counters | unit 0-0 counters | cpu data-plane statistics | cpu i2c statistics | cpu party-bus statistics | cpu sata-interface statistics | stack-port 0-127}`

Parameters	stack-unit <i>id</i>	Enter the keywords <code>stack-unit</code> then a number to select a particular stack member and then enter one of the following command options to clear a specific collection of data. The range is from 1 to 6.
	counters	Enter the keyword <code>counters</code> to clear the counters on the selected stack member.
	unit <i>number</i> counters	Enter the keyword <code>unit</code> along with a port-pipe number, then the keyword <code>counters</code> to clear the counters on the selected port-pipe. The range is from 0 to 0.
	cpu data-plane statistics	Enter the keywords <code>cpu data-plane statistics</code> to clear the data plane statistics.
	cpu party-bus statistics	Enter the keywords <code>cpu party-bus statistics</code> to clear the management statistics.
	stack-port	Enter the keywords <code>stack-port</code> then the port number of the stacking port to clear the statistics of the particular stacking port. The range is from 1 to 128.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	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 stack-unit](#) — 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 selected hardware components.

Syntax `clear hardware system-flow layer2 stack-unit number port-set 0-0 counters`

Parameters

stack-unit <i>number</i>	Enter the keywords <code>stack-unit</code> then a number to select a particular stack member and then enter one of the following command options to clear a specific collection of data. The range is from 1 to 6.
port-set 0-0 counters	Enter the keywords <code>port-set</code> along with a port-pipe number, then the keyword <code>counters</code> to clear the system-flow counters on the selected port-pipe. The range is from 0 to 0.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	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 stack-unit](#) — displays the data plane or management plane input and output statistics of the designated component of the designated stack member.

clear hardware vlan-counters

Clear VLAN statistics.

Syntax `clear hardware vlan-counters vlan-id`

Parameters

<i>vlan-id</i>	Enter the interface VLAN number. The range is from 1 to 4094.

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
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Introduced this command.

hardware watchdog

To trigger a reboot and restart the system, set the watchdog timer.

Syntax	<code>hardware watchdog stack-unit {<0-5> all}</code>
Defaults	Enabled.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
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.

Usage Information	This command enables a hardware watchdog mechanism that automatically reboots an Dell Networking OS switch/ router with a single unresponsive unit. This behavior is a last-resort mechanism intended to prevent a manual power cycle.

show hardware layer2

Display Layer 2 ACL or eg data for the selected stack member and stack member port-pipe.

Syntax	<code>show hardware layer2 {eg-acl in-acl} stack-unit id port-set 0-0</code>	
Parameters	eg-acl in-acl	Enter either the keyword <code>eg-acl</code> or the keyword <code>in-acl</code> to select between ingress or egress ACL data.
	stack-unit id	Enter the keyword <code>stack-unit</code> to select a stack ID. The range is from 1 to 6.
	port-set 0-0	Enter the keywords <code>port-set</code> with a port-pipe number. . The range is from 0 to 0.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	



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.
9.0.2.0	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.

Usage Information The unit numbers given are internal port numbers.

show hardware layer3

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

Syntax `show hardware layer3 {acl | qos} stack-unit number port-set 0-0`

Parameters

acl qos	Enter either the keyword <code>acl</code> or the keyword <code>qos</code> to select between ACL or QoS data.
stack-unit <i>number</i>	Enter the keywords <code>stack-unit</code> then a number to select a stack ID. The range is from 1 to 6.
port-set <i>0-0</i>	Enter the keyword <code>port-set</code> with a port-pipe number. The range is from 0 to 0.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
7.8.1.0	Introduced on the S-Series.



show hardware stack-unit

Display the data plane or management plane input and output statistics of the designated component of the designated stack member.

Syntax

```
stack-unit <id> {buffer [ unit 0 ] total buffer | buffer unit 0 interface  
all queue [(0-14) | all] buffer-info}{cpu data-plane statistics | cpu  
management statistics | drops [unit number] | fpga register | party-bus  
statistics | stack-port | ti-monitor | unit 0-1 {counters | details | port-  
stats [detail] | register}}
```

Parameters

stack-unit stack-unit {command-option}

Enter the keywords `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. The range is from 1 to 6.

buffer

Enter the keyword `buffer`. To display the total buffer statistics for the stack unit, enter the keyword `total-buffer`. To display buffer statistics for a all interface, enter the keyword `interface` followed by the keyword `all`.

To display total buffer information for the port, enter the keywords `buffer-info`. To display a queue range, enter 0 to 14 for a specific queue or `all`.

cpu data-plane statistics

(Optional) Enter the keywords `cpu data-plane statistics` then the keywords `stack port` and its number, from 1 to 128 to display the data plane statistics, which shows the High Gig (Higig) port raw input/output counter statistics to which the stacking module is connected.

cpu management statistics

Enter the keywords `cpu management statistics` to display the counters of the management port.

cpu party-bus statistics

Enter the keywords `cpu party-bus statistics`, to display the Management plane input/output counter statistics of the pseudo party bus interface.

drops [unit unit-number]

Enter the keyword `drops` to display internal drops on the selected stack member. Enter the drops keyword to display internal drops on the selected stack member.

fpga register

Enter the keyword to display the register value of fpga register details in S4810, Z9000 and S6000.

unit unit-number {counters | details | port-stats [detail] | register}

Enter the keyword `unit` then 0 to 3 and then enter one of the following keywords to troubleshoot errors on the selected port-pipe and to give status on why a port is not coming up to register level: `counters`, `details`, `port-stats [detail]`, or `register`.

TI monitor

Enter the unit keyword to show information regarding the TI register.

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
9.8(0.0)	Replaced the keyword <code>port</code> with <code>interface</code> .
9.7(0.0)	Introduced on the S6000-ON.
9.2(0.2)	Modified the <code>drops</code> keyword range, unit keyword range and added the <code>buffer</code> and <code>cpu management statistics</code> options.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.5	Added <code>i2c</code> statistics and <code>sata-interfaces</code> 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.
7.7.1.0	Introduced on the S-Series.

Example (Data-Plane)

```
Dell#show hardware stack-unit 1 cpu data-plane statistics
Input Statistics:
 1856 packets, 338262 bytes
 141 64-byte pkts, 1248 over 64-byte pkts, 11 over 127-byte pkts
 222 over 255-byte pkts, 236 over 511-byte pkts, 0 over 1023-byte pkts
 919 Multicasts, 430 Broadcasts
 0 runs, 0 giants, 0 throttles
 0 CRC, 0 overrun, 0 discarded
Output Statistics:
 325 packets, 27629 bytes, 0 underruns
 9 64-byte pkts, 310 over 64-byte pkts, 1 over 127-byte pkts
 1 over 255-byte pkts, 2 over 511-byte pkts, 2 over 1023-byte pkts
 0 Multicasts, 3 Broadcasts, 322 Unicasts
 0 throttles, 0 discarded, 0 collisions
Rate info (interval 299 seconds):
 Input 00.00 Mbits/sec
 Output 00.00 Mbits/sec
Dell#
```

Example (Party-Bus)

```
Dell#show hardware stack-unit 1 cpu party-bus statistics
Input Statistics:
 8189 packets, 8076608 bytes
 0 dropped, 0 errors
Output Statistics:
 366 packets, 133100 bytes
 0 errors
Dell#
```

Example (Drops Unit)

```
Dell#sh hard stack-unit 1 drops unit 0
PortNumberIngress Drops IngMac Drops Total Mmu Drops
1          0          0          0
2          0          0          0
3          0          0          0
4          0          0          0
EgMac Drops Egress Drops
0          0
0          0
0          0
0          0
Dell#
```



Example (Port-Stats)

```
Dell#show hardware stack-unit 1 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
ge0 down - SW Yes Block Untag FA SGMII 1554
ge1 !ena - SW Yes Block Tag FA SGMII 1554
ge2 !ena - SW Yes Block Tag FA SGMII 1554
ge3 !ena - SW Yes Block Tag FA SGMII 1554
ge4 !ena - SW Yes Forward Tag F SGMII 1554
ge5 !ena - SW Yes Forward Tag F SGMII 1554
ge6 !ena - SW Yes Forward Tag F SGMII 1554
ge7 !ena - SW Yes Forward Tag F SGMII 1554
ge8 !ena - SW Yes Forward Tag F SGMII 1554
ge9 !ena - SW Yes Forward Tag F SGMII 1554
ge10 !ena - SW Yes Forward Tag F SGMII 9252
ge11 !ena - SW Yes Forward Tag F SGMII 9252
ge12 !ena - SW Yes Forward Tag F SGMII 1554
ge13 !ena - SW Yes Forward Tag F SGMII 1554
ge14 !ena - SW Yes Forward Tag F SGMII 1554
ge15 !ena - SW Yes Forward Tag F SGMII 1554
ge16 !ena - SW Yes Forward Tag F SGMII 1554
ge17 !ena - SW Yes Forward Tag F SGMII 1554
ge18 !ena - SW Yes Forward Tag F SGMII 1554
ge19 !ena - SW Yes Forward Tag F SGMII 1554
ge20 !ena - SW Yes Forward Tag F SGMII 1554
ge21 !ena - SW Yes Forward Tag F SGMII 1554
ge22 !ena - SW Yes Forward Tag F SGMII 1554
ge23 !ena - SW Yes Forward Tag F SGMII 1554
hg0 up 12G FD SW No Forward None F XGMII 16360
hg1 up 12G FD SW No Forward None F XGMII 16360
hg2 down 10G FD SW No Forward None F XGMII 16360
hg3 down 10G FD SW No Forward None F XGMII 16360
0
Dell#
```

Example (Register)

```
Dell#show hardware stack-unit 1 unit 1 register
0x0068003c AGINGCTRMEMDEBUG.mmu0 = 0x00000000
0x0068003d AGINGEXPMEMDEBUG.mmu0 = 0x00000000
0x00680017 ASFCONFIG.mmu0 = 0x0000000e
0x0060004c ASFPORTSPEED.ge0 = 0x00000000
0x0060104c ASFPORTSPEED.ge1 = 0x00000000
0x0060204c ASFPORTSPEED.ge2 = 0x00000000
0x0060304c ASFPORTSPEED.ge3 = 0x00000000
0x0060404c ASFPORTSPEED.ge4 = 0x00000000
0x0060504c ASFPORTSPEED.ge5 = 0x00000000
0x0060604c ASFPORTSPEED.ge6 = 0x00000000
0x0060704c ASFPORTSPEED.ge7 = 0x00000000
0x0060804c ASFPORTSPEED.ge8 = 0x00000000
0x0060904c ASFPORTSPEED.ge9 = 0x00000000
0x0060a04c ASFPORTSPEED.ge10 = 0x00000000
0x0060b04c ASFPORTSPEED.ge11 = 0x00000000
0x0060c04c ASFPORTSPEED.ge12 = 0x00000000
0x0060d04c ASFPORTSPEED.ge13 = 0x00000000
0x0060e04c ASFPORTSPEED.ge14 = 0x00000000
0x0060f04c ASFPORTSPEED.ge15 = 0x00000000
0x0061004c ASFPORTSPEED.ge16 = 0x00000000
0x0061104c ASFPORTSPEED.ge17 = 0x00000000
0x0061204c ASFPORTSPEED.ge18 = 0x00000000
0x0061304c ASFPORTSPEED.ge19 = 0x00000000
0x0061404c ASFPORTSPEED.ge20 = 0x00000000
0x0061504c ASFPORTSPEED.ge21 = 0x00000000
0x0061604c ASFPORTSPEED.ge22 = 0x00000000
0x0061704c ASFPORTSPEED.ge23 = 0x00000005
0x0061804c ASFPORTSPEED.hg0 = 0x00000007
0x0061904c ASFPORTSPEED.hg1 = 0x00000007
0x0061a04c ASFPORTSPEED.hg2 = 0x00000000
0x0061b04c ASFPORTSPEED.hg3 = 0x00000000
0x0061c04c ASFPORTSPEED.cpu0 = 0x00000000
0x00780000 AUX_ARB_CONTROL.ipipe0 = 0x0000001c
```



```

0x0e700102 BCAST_BLOCK_MASK.ge0 = 0x00000000
0x0e701102 BCAST_BLOCK_MASK.ge1 = 0x00000000
0x0e702102 BCAST_BLOCK_MASK.ge2 = 0x00000000
0x0e703102 BCAST_BLOCK_MASK.ge3 = 0x00000000
0x0e704102 BCAST_BLOCK_MASK.ge4 = 0x00000000
0x0e705102 BCAST_BLOCK_MASK.ge5 = 0x00000000
0x0e706102 BCAST_BLOCK_MASK.ge6 = 0x00000000
0x0e707102 BCAST_BLOCK_MASK.ge7 = 0x00000000
0x0e708102 BCAST_BLOCK_MASK.ge8 = 0x00000000
0x0e709102 BCAST_BLOCK_MASK.ge9 = 0x00000000
0x0e70a102 BCAST_BLOCK_MASK.ge10 = 0x00000000
0x0e70b102 BCAST_BLOCK_MASK.ge11 = 0x00000000
0x0e70c102 BCAST_BLOCK_MASK.ge12 = 0x00000000
0x0e70d102 BCAST_BLOCK_MASK.ge13 = 0x00000000
0x0e70e102 BCAST_BLOCK_MASK.ge14 = 0x00000000
0x0e70f102 BCAST_BLOCK_MASK.ge15 = 0x00000000
0x0e710102 BCAST_BLOCK_MASK.ge16 = 0x00000000
0x0e711102 BCAST_BLOCK_MASK.ge17 = 0x00000000
0x0e712102 BCAST_BLOCK_MASK.ge18 = 0x00000000
0x0e713102 BCAST_BLOCK_MASK.ge19 = 0x00000000
0x0e714102 BCAST_BLOCK_MASK.ge20 = 0x00000000
0x0e715102 BCAST_BLOCK_MASK.ge21 = 0x00000000
0x0e716102 BCAST_BLOCK_MASK.ge22 = 0x00000000
0x0e717102 BCAST_BLOCK_MASK.ge23 = 0x00000000
0x0e718102 BCAST_BLOCK_MASK.hg0 = 0x00000000
0x0e719102 BCAST_BLOCK_MASK.hg1 = 0x00000000
0x0e71a102 BCAST_BLOCK_MASK.hg2 = 0x00000000
0x0e71b102 BCAST_BLOCK_MASK.hg3 = 0x00000000
0x0e71c102 BCAST_BLOCK_MASK.cpu0 = 0x00000000
0x0b700001 BCAST_STORM_CONTROL.ge0 = 0x00000000
0x0b701001 BCAST_STORM_CONTROL.ge1 = 0x00000000
0x0b702001 BCAST_STORM_CONTROL.ge2 = 0x00000000
0x0b703001 BCAST_STORM_CONTROL.ge3 = 0x00000000
0x0b704001 BCAST_STORM_CONTROL.ge4 = 0x00000000
0x0b705001 BCAST_STORM_CONTROL.ge5 = 0x00000000
0x0b706001 BCAST_STORM_CONTROL.ge6 = 0x00000000
0x0b707001 BCAST_STORM_CONTROL.ge7 = 0x00000000
0x0b708001 BCAST_STORM_CONTROL.ge8 = 0x00000000
0x0b709001 BCAST_STORM_CONTROL.ge9 = 0x00000000
0x0b70a001 BCAST_STORM_CONTROL.ge10 = 0x00000000
!----- output truncated -----!

```

Example (Counters)

```

Dell#show hardware stack-unit 1 unit 0 counters
unit: 0 port: 1 (interface Te 1/1/1)
Description                                     Value
RX - IPV4 L3 Unicast Frame Counter              0
RX - IPV4 L3 Routed Multicast Packets            0
RX - IPV6 L3 Unicast Frame Counter              0
RX - IPV6 L3 Routed Multicast Packets            0
RX - Unicast Packet Counter                     0
RX - 64 Byte Frame Counter                      336186
RX - 65 to 127 Byte Frame Counter                0
RX - 128 to 255 Byte Frame Counter               0
RX - 256 to 511 Byte Frame Counter               0
RX - 512 to 1023 Byte Frame Counter              0
RX - 1024 to 1518 Byte Frame Counter             0
RX - 1519 to 1522 Byte Good VLAN Frame Counter  0
RX - 1519 to 2047 Byte Frame Counter            0
RX - 2048 to 4095 Byte Frame Counter            0
RX - 4096 to 9216 Byte Frame Counter            0
RX - Good Packet Counter                       336186
RX - Packet/Frame Counter                     336186
RX - Unicast Frame Counter                     0
RX - Multicast Frame Counter                   336186
RX - Broadcast Frame Counter                   0
RX - Byte Counter                             21515904
RX - Control Frame Counter                     0

```



RX - Pause Control Frame Counter	0
RX - Oversized Frame Counter	0
RX - Jabber Frame Counter	0
RX - VLAN Tag Frame Counter	0
RX - Double VLAN Tag Frame Counter	0
RX - RUNT Frame Counter	0
RX - Fragment Counter	0
RX - VLAN Tagged Packets	0
RX - Ingress Dropped Packet	0
RX - MTU Check Error Frame Counter	0
RX - PFC Frame Priority 0	0
RX - PFC Frame Priority 1	0
RX - PFC Frame Priority 2	0
RX - PFC Frame Priority 3	0
RX - PFC Frame Priority 4	0
RX - PFC Frame Priority 5	0
RX - PFC Frame Priority 6	0
RX - PFC Frame Priority 7	0
RX - Debug Counter 0	336186
RX - Debug Counter 1	336186
RX - Debug Counter 2	0
RX - Debug Counter 3	0
RX - Debug Counter 4	0
RX - Debug Counter 5	336186
RX - Debug Counter 6	0
RX - Debug Counter 7	0
RX - Debug Counter 8	0
TX - 64 Byte Frame Counter	166
TX - 65 to 127 Byte Frame Counter	112
TX - 128 to 255 Byte Frame Counter	0
TX - 256 to 511 Byte Frame Counter	0
TX - 512 to 1023 Byte Frame Counter	0
TX - 1024 to 1518 Byte Frame Counter	0
TX - 1519 to 1522 Byte Good VLAN Frame Counter	0
TX - 1519 to 2047 Byte Frame Counter	0
TX - 2048 to 4095 Byte Frame Counter	0
TX - 4096 to 9216 Byte Frame Counter	0
TX - Good Packet Counter	278
TX - Packet/Frame Counter	278
TX - Unicast Frame Counter	0
TX - Multicast Frame Counter	278
TX - Broadcast Frame Counter	0
TX - Byte Counter	18688
TX - Control Frame Counter	0
TX - Pause Control Frame Counter	0
TX - Oversized Frame Counter	0
TX - Jabber Counter	0
TX - VLAN Tag Frame Counter	0
TX - Double VLAN Tag Frame Counter	0
TX - RUNT Frame Counter	0
TX - Fragment Counter	0
TX - PFC Frame Priority 0	0
TX - PFC Frame Priority 1	0
TX - PFC Frame Priority 2	0
TX - PFC Frame Priority 3	0
TX - PFC Frame Priority 4	0
TX - PFC Frame Priority 5	0
TX - PFC Frame Priority 6	0
TX - PFC Frame Priority 7	0
TX - Debug Counter 0	0
TX - Debug Counter 1	0
TX - Debug Counter 2	0
TX - Debug Counter 3	0
TX - Debug Counter 4	0
TX - Debug Counter 5	0
TX - Debug Counter 6	0
TX - Debug Counter 7	0
TX - Debug Counter 8	0
TX - Debug Counter 9	0



```

TX - Debug Counter 10                                0
TX - Debug Counter 11                                0

-----
-----
-----
-----
-----
unit: 0 port: 61 (interface Fo 1/60/1)
Description                                           Value

RX - IPv4 L3 Unicast Frame Counter                    0
RX - IPv4 L3 Routed Multicast Packets                  0
RX - IPv6 L3 Unicast Frame Counter                    0
RX - IPv6 L3 Routed Multicast Packets                  0
RX - Unicast Packet Counter                          0
RX - 64 Byte Frame Counter                            0
RX - 65 to 127 Byte Frame Counter                      0
RX - 128 to 255 Byte Frame Counter                    0
RX - 256 to 511 Byte Frame Counter                    0
RX - 512 to 1023 Byte Frame Counter                    0
RX - 1024 to 1518 Byte Frame Counter                   0
RX - 1519 to 1522 Byte Good VLAN Frame Counter        0
RX - 1519 to 2047 Byte Frame Counter                   0
RX - 2048 to 4095 Byte Frame Counter                   0
RX - 4096 to 9216 Byte Frame Counter                   0
RX - Good Packet Counter                              0
RX - Packet/Frame Counter                             0
RX - Unicast Frame Counter                            0
RX - Multicast Frame Counter                          0
RX - Broadcast Frame Counter                          0
RX - Byte Counter                                     0
RX - Control Frame Counter                            0
RX - Pause Control Frame Counter                      0
RX - Oversized Frame Counter                          0
RX - Jabber Frame Counter                             0
RX - VLAN Tag Frame Counter                           0
RX - Double VLAN Tag Frame Counter                    0
RX - RUNT Frame Counter                               0
RX - Fragment Counter                                 0
RX - VLAN Tagged Packets                              0
RX - Ingress Dropped Packet                           0
RX - MTU Check Error Frame Counter                    0
RX - PFC Frame Priority 0                             0
RX - PFC Frame Priority 1                             0
RX - PFC Frame Priority 2                             0
RX - PFC Frame Priority 3                             0
RX - PFC Frame Priority 4                             0
RX - PFC Frame Priority 5                             0
RX - PFC Frame Priority 6                             0
RX - PFC Frame Priority 7                             0
RX - Debug Counter 0                                  0
RX - Debug Counter 1                                  0
RX - Debug Counter 2                                  0
RX - Debug Counter 3                                  0
RX - Debug Counter 4                                  0
RX - Debug Counter 5                                  0
RX - Debug Counter 6                                  0
RX - Debug Counter 7                                  0
RX - Debug Counter 8                                  0
TX - 64 Byte Frame Counter                            0
TX - 65 to 127 Byte Frame Counter                      0
TX - 128 to 255 Byte Frame Counter                    0
TX - 256 to 511 Byte Frame Counter                    0
TX - 512 to 1023 Byte Frame Counter                    0
TX - 1024 to 1518 Byte Frame Counter                   0
TX - 1519 to 1522 Byte Good VLAN Frame Counter        0
TX - 1519 to 2047 Byte Frame Counter                   0
TX - 2048 to 4095 Byte Frame Counter                   0

```



```

TX - 4096 to 9216 Byte Frame Counter      0
TX - Good Packet Counter                  0
TX - Packet/Frame Counter                 0
TX - Unicast Frame Counter                0
TX - Multicast Frame Counter              0
TX - Broadcast Frame Counter              0
TX - Byte Counter                        0
TX - Control Frame Counter                0
TX - Pause Control Frame Counter          0
TX - Oversized Frame Counter             0
TX - Jabber Counter                      0
TX - VLAN Tag Frame Counter              0
TX - Double VLAN Tag Frame Counter        0
TX - RUNT Frame Counter                  0
TX - Fragment Counter                    0
TX - PFC Frame Priority 0                 0
TX - PFC Frame Priority 1                 0
TX - PFC Frame Priority 2                 0
TX - PFC Frame Priority 3                 0
TX - PFC Frame Priority 4                 0
TX - PFC Frame Priority 5                 0
TX - PFC Frame Priority 6                 0
TX - PFC Frame Priority 7                 0
TX - Debug Counter 0                     0
TX - Debug Counter 1                     0
TX - Debug Counter 2                     0
TX - Debug Counter 3                     0
TX - Debug Counter 4                     0
TX - Debug Counter 5                     0
TX - Debug Counter 6                     0
TX - Debug Counter 7                     0
TX - Debug Counter 8                     0
TX - Debug Counter 9                     0
TX - Debug Counter 10                    0
TX - Debug Counter 11                    0

```

Example (Details)

```

Dell#show hardware stack-unit 1 unit 1 details

*****

The total no of FP & CSF Devices in the Card is 2
The total no of FP Devices in the Card is 2
The total no of CSF Devices in the Card is 0
The number of ports in device 0 is - 24
The number of Hg ports in devices 0 is - 4
The CPU Port of the device is 28
The number of ports in device 1 is - 24
The number of Hg ports in devices 1 is - 4
The CPU Port of the device is 28
The staring unit no the SWF in the device is 0
*****

The Current Link Status Is

Front End Link Status 0x000000000000400000000000
Front End Port Present Status 0x000000000000000000000000
Back Plane Link Status 0x00000000

*****

Link Status of all the ports in the Device - 1
The linkStatus of Front End Port 0 is FALSE
The linkStatus of Front End Port 1 is FALSE
The linkStatus of Front End Port 2 is FALSE
The linkStatus of Front End Port 3 is FALSE
The linkStatus of Front End Port 4 is FALSE
The linkStatus of Front End Port 5 is FALSE
The linkStatus of Front End Port 6 is FALSE

```



```

The linkStatus of Front End Port 7 is FALSE
The linkStatus of Front End Port 8 is FALSE
The linkStatus of Front End Port 9 is FALSE
The linkStatus of Front End Port 10 is FALSE
The linkStatus of Front End Port 11 is FALSE
The linkStatus of Front End Port 12 is FALSE
The linkStatus of Front End Port 13 is FALSE
The linkStatus of Front End Port 14 is FALSE
The linkStatus of Front End Port 15 is FALSE
The linkStatus of Front End Port 16 is FALSE
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 FALSE
The linkStatus of Front End Port 22 is FALSE
The linkStatus of Front End Port 23 is TRUE
The linkStatus of Hg Port 24 is TRUE
The linkStatus of Hg Port 25 is TRUE
The linkStatus of Hg Port 26 is FALSE
The linkStatus of Hg Port 27 is FALSE
!----- output truncated -----!

```

Example (Total-Buffer)

```

Dell#show hardware stack-unit 1 buffer total-buffer

Dell#show hardware stack-unit 1 buffer total-buffer
----- Buffer Details for Stack-Unit 1 -----
Total Buffers allocated per Stack-Unit 46080

```

Example displaying queue range

```

Dell#show hardware stack-unit 0 buffer unit 0 interface all queue 6 buffer-
info
      Buffer Stats for Front End Ports
      =====
----- Buffer Stats for Interface Te 1/1/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/2/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/3/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/4/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/5/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/6/1 Queue 6 -----
<output truncated for brevity>

```

Related Commands

[clear hardware system-flow](#) — clears the statistics from selected hardware components.

[show interfaces stack-unit](#) — displays information on all interfaces on a specific S-Series stack member.



[show system \(S-Series and Z-Series\)](#) — displays the current status of all the stack members or a specific member.

show hardware stack-unit buffer

Display the counters for the specified port, minimum guaranteed buffer of a priority-group, and the shared buffer.

Syntax

```
show hardware stack-unit <0-5> buffer unit <0-0> port {1-104 | all}
priority-group <0 -7> buffer-info
show hardware stack-unit {id} buffer unit {id} interface all {priority-group
{ id | all } | queue { id| all} ] buffer-info
```

Parameters

stack-unit <0-5>	Enter the keywords <code>stack-unit</code> 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. The range is from 1 to 5.
buffer unit <0-5>	Enter the keyword <code>buffer</code> . To display the total buffer statistics for the stack unit, enter the keyword <code>total-buffer</code> . To display the buffer statistics for a specific unit, enter the keyword <code>unit</code> and a unit number 0 .
interface <i>interface</i>	Enter the keyword <code>interface</code> followed by the keyword <code>all</code> to display buffer statistics for all interface. Enter any of the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
port	To display the buffer statistics for a specific port, enter the keyword <code>port</code> and a port number from 1 to 64.
all	Display buffer statistics for all ports
queue	Enter the keyword <code>queue</code> followed by <code>id</code> for specific queue or keyword <code>all</code> .
priority-group	Identifier of the priority group in the range of 0 to 7. Enter the keyword <code>priority-group</code> followed by <code>{id}</code> for specific priority group or keyword <code>all</code> .
buffer-info	To display total buffer information for the port interface, enter the keywords <code>buffer-info</code> . To display a queue range, enter 0 to 14 for a specific queue or <code>all</code> .

Command Modes

EXEC

EXEC Privilege

Command History

Version	Description
9.8(0.0)	Removed the keyword <code>port</code> and added the keywords <code>interface</code> , and the variable <code>interface</code> .
9.7(0.0)	Introduced on the S6000-ON.



Version	Description
Version 9.3(0.0)	Introduced on the S6000 platform.

Usage Information The following table describes the fields in the output of the show command:

Field	Description
Buffer Accounting Stats for Unit 0 Port 1 priority-group 0	Displays the counters that are calculated by the buffer statistics tracking method for each port per priority group on a particular stack member.
Max Shared Limit	Maximum shared buffer space allotted to the specific port for the corresponding stack unit
Default Packet Buffer allocate for the priority-group	The default packet buffer size in KB that is associated with the particular priority group
Accounted Packet Buffer	Shared buffer space that is in use by the packets

Example

```
Dell# show hardware stack-unit 1 buffer unit 0 port 1 priority-group 0
buffer-info

----- Buffer Accounting Stats for Unit 0Port 1 priority-group 0 -----
Maximum Shared Limit: 0
Default Packet Buffer allocate for the priority-group: 61440
Accounted Packet Buffer: 0
```

Example displaying total-buffer information for all interface in the specified stack member and unit

```
Dell#show hardware stack-unit 0 buffer unit 0 interface all buffer-info

          Buffer Stats for Front End Ports
          =====
----- Buffer Stats for Interface Te 1/1/1 -----
Maximum Shared Limit for the Interface: 38336
Default Packet Buffer allocate for the Interface: 120
Used Packet Buffer for the Interface: 0
----- Buffer Stats for Interface Te 1/1/1 -----
Maximum Shared Limit for the Interface: 38336
Default Packet Buffer allocate for the Interface: 120
Used Packet Buffer for the Interface: 0
----- Buffer Stats for Interface Te 1/2/1 -----
Maximum Shared Limit for the Interface: 38336
Default Packet Buffer allocate for the Interface: 120
Used Packet Buffer for the Interface: 0
----- Buffer Stats for Interface Te 1/3/1 -----
Maximum Shared Limit for the Interface: 38336
Default Packet Buffer allocate for the Interface: 120
Used Packet Buffer for the Interface: 0
----- Buffer Stats for Interface Te 1/4/1 -----
Maximum Shared Limit for the Interface: 38336
Default Packet Buffer allocate for the Interface: 120
Used Packet Buffer for the Interface: 0
----- Buffer Stats for Interface Te 1/5/1 -----
Maximum Shared Limit for the Interface: 38336
Default Packet Buffer allocate for the Interface: 120
Used Packet Buffer for the Interface: 0
----- Buffer Stats for Interface Te 1/6/1-----
<output truncated for brevity>
```

Example displaying queue range

```
Dell#show hardware stack-unit 0 buffer unit 0 interface all queue 6 buffer-
info

          Buffer Stats for Front End Ports
          =====
----- Buffer Stats for Interface Te 1/1/1 Queue 6 -----
```




```

Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/1/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/2/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/3/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/4/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/5/1 Queue 6 -----
Maximum Shared Limit: 7667
Default Packet Buffer allocate for the Queue: 8
Used Packet Buffer: 0
----- Buffer Stats for Interface Te 1/6/1 Queue 6 -----
<output truncated for brevity>

```

show hardware buffer-stats-snapshot

Displays buffer statistics tracking resource information for a specific interface.

Syntax

```
show hardware buffer-stats-snapshot resource interface interface{priority-
group { id | all } | queue { ucast{id | all}{ mcast {id | all} | all}}
```

Parameters

buffer-stats-snapshot unit <i>number</i>	Display the historical snapshot of buffer statistical values unit Enter the keyword <i>unit</i> along with a port-pipe number. The range is from 0 to 0.
interface <i>interface</i>	Enter any of the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
queue	Enter the keyword <code>queue</code> after <i>id</i> for specific queue or keyword <code>all</code> .
priority-group	Enter the keyword <code>priority-group</code> followed by <i>id</i> for specific priority-group or keyword <i>all</i> .

Command Modes

EXEC
EXEC Privilege

Command History

Version	Description
9.8(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, Z9000, Z9500.



Usage Information <Interface><slot/port>-Queue ucast/mcast — Displays the total unicast/multicast buffer usage on per-port per-queue basis. For CPU port, counters for queues 0 to 11 displays and there is no differentiation between unicast and multicast queues.

Example displaying egress queue-level snapshot for both unicast and multicast packets for the specific interface

```
Dell# show hardware buffer-stats-snapshot resource interface fortyGigE 1/1
queue all
Unit 1 unit: 0 port: 1 (interface Fo 1/1)
```

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

Example displaying egress queue-level snapshot for unicast packets for the specific interface

```
Del#show hardware buffer-stats-snapshot resource interface fortyGigE 1/1
queue ucast 10
Unit 1 unit: 0 port: 1 (interface Fo 1/1)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
UCAST		10	0

```
Dell#show hardware buffer-stats-snapshot resource interface fortyGigE 1/1
queue ucast all
Unit 1 unit: 0 port: 1 (interface Fo 1/1)
```

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

Example displaying egress queue-level snapshot for multicast packets for the specific interface

```
Dell#show hardware buffer-stats-snapshot resource interface fortyGigE 1/1
queue mcast 3
Unit 0 unit: 0 port: 1 (interface Fo 1/1)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS



```

-----
MCAST          3          0

Dell#show hardware buffer-stats-snapshot resource interface fortyGigE 1/1
queue mcast all

Unit 1 unit: 0 port: 1 (interface Fo 1/1)
-----
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

```

**Example displaying
ingress priority-
group level snapshot
for the specific
interface**

```

Dell#show hardware buffer-stats-snapshot resource interface fortyGigE 1/1
priority-group 7

Unit 1 unit: 0 port: 1 (interface Fo 1/1)
-----
PG#      SHARED CELLS      HEADROOM CELLS
-----
7         0                 0

Dell#show hardware buffer-stats-snapshot resource interface fortyGigE 1/1
priority-group all

Unit 1 unit: 0 port: 1 (interface Fo 1/1)
-----
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

```

show hardware counters interface

Display the counter information for a specific interface.

Syntax `show hardware counters interface interface`

Parameters

- counters** Enter the keywords `counters` to display counter value for the specified stack-member the port-pipe.
- interface *interface*** Enter any of the following keywords and slot/port[/subport] or number 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.

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
9.8(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, Z9500.

Example

```
Dell#show hardware counters interfac tengigabitethernet 5/1/1
unit: 0 port: 2 (interface Te 5/1/1)
Description                                     Value
RX - IPv4 L3 Unicast Frame Counter              0
RX - IPv4 L3 Routed Multicast Packets           0
RX - IPv6 L3 Unicast Frame Counter              0
RX - IPv6 L3 Routed Multicast Packets           0
RX - Unicast Packet Counter                     0
RX - 64 Byte Frame Counter                      0
RX - 65 to 127 Byte Frame Counter               0
RX - 128 to 255 Byte Frame Counter              0
RX - 256 to 511 Byte Frame Counter              0
RX - 512 to 1023 Byte Frame Counter             0
RX - 1024 to 1518 Byte Frame Counter            0
RX - 1519 to 1522 Byte Good VLAN Frame Counter 0
RX - 1519 to 2047 Byte Frame Counter            0
RX - 2048 to 4095 Byte Frame Counter            0
RX - 4096 to 9216 Byte Frame Counter            0
RX - Good Packet Counter                       0
RX - Packet/Frame Counter                      0
RX - Unicast Frame Counter                     0
RX - Multicast Frame Counter                   0
RX - Broadcast Frame Counter                   0
RX - Byte Counter                             0
RX - Control Frame Counter                     0
RX - Pause Control Frame Counter               0
RX - Oversized Frame Counter                   0
RX - Jabber Frame Counter                      0
RX - VLAN Tag Frame Counter                    0
RX - Double VLAN Tag Frame Counter             0
RX - RUNT Frame Counter                       0
RX - Fragment Counter                         0
RX - VLAN Tagged Packets                       0
RX - Ingress Dropped Packet                   0
RX - MTU Check Error Frame Counter             0
RX - PFC Frame Priority 0                      0
RX - PFC Frame Priority 1                      0
RX - PFC Frame Priority 2                      0
RX - PFC Frame Priority 3                      0
RX - PFC Frame Priority 4                      0
RX - PFC Frame Priority 5                      0
RX - PFC Frame Priority 6                      0
RX - PFC Frame Priority 7                      0
RX - Debug Counter 0                          0
RX - Debug Counter 1                          0
RX - Debug Counter 2                          0
<output truncated for brevity>
```



show hardware drops

Displays internal drops on the specified interface or for a range of interface.

Syntax `show hardware drops interface interface`

Parameters

interface	Enter any of the following keywords and slot/port[/subport] or slot/port-range or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
drops	Enter the keyword <code>drops</code> to display internal drops.

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
9.8(0.0)	Removed the keywords <code>stack-unit</code> . Introduced on the Z9500.
9.7(0.0)	Introduced on the S6000-ON.
9.2(0.2)	Modified the <code>drops</code> keyword <code>range</code> , unit keyword <code>range</code> and added the <code>buffer</code> and <code>cpu management statistics</code> options.
9.0.2.0	Introduced on the S6000.
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.
7.7.1.0	Introduced on the S-Series.

Example displaying internal drops for the specific interface

```
Dell#show hardware drops interface tengigabitethernet 2/1/1
Drops in Interface Te 2/1/1:
  --- Ingress Drops      ---
Ingress Drops            : 0
IBP CBP Full Drops       : 0
PortSTPnotFwd Drops     : 0
IPv4 L3 Discards         : 0
Policy Discards          : 0
```



```

Packets dropped by FP          : 0
(L2+L3) Drops                 : 0
Port bitmap zero Drops        : 0
Rx VLAN Drops                 : 0
--- Ingress MAC counters---
Ingress FCS Drops             : 0
Ingress MTUExceeds           : 0
--- MMU Drops ---
Ingress MMU Drops             : 0
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
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

```

show hardware system-flow

Display Layer 3 ACL or QoS data for the selected stack member and stack member port-pipe.

Syntax	<code>show hardware system-flow layer2 stack-unit <i>id</i> port-set <i>number</i> [counters]</code>	
Parameters	acl qos	For the selected stack member and stack member port-pipe, display which system flow entry the packet hits and what queue the packet takes as it dumps the raw system flow tables.
	stack-unit <i>id</i>	Enter the keywords <code>stack-unit</code> to select a stack member ID. The range is from 1 to 6.
	port-set <i>number</i> [counters]	Enter the keywords <code>port-set</code> with a port-pipe number.
		The range is from 0 to 0.



(OPTIONAL) Enter the keyword `counters` to display hit counters for the selected ACL or QoS option.

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
9.7(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.

Example

```
Dell#show hardware system-flow layer2 stack-unit 1 port-set 0 counters
```

EntryId	Description	#HITS
2048	STP BPDU Redirects	0
2047	LLDP BPDU Redirects	0
2045	LACP traffic Redirects	0
2044	GVRP traffic Redirects	0
2043	ARP Reply Redirects	0
2042	802.1x frames Redirects	0
2041	VRRP frames Redirects	0
2040	GRAT ARP	0
2039	DROP Cases	0
2038	OSPF1 STUB	0
2037	OSPF2 STUB	0
2036	VRRP STUB	0
2035	L2_DST_HIT+BC MAC+VLAN 4095	0
2034	L2_DST_HIT+BC MAC	0
2033	Catch all	0
384	OSPF[224.0.0.5] Packets	0
383	OSPF[224.0.0.6] Packets	0
382	VRRP Packets	0
380	BCast L2_DST_HIT on VLAN 4095	0
379	BCAST L2_DST_HIT Packets	0
4	Unknown L2MC Packets	0
3	L2DLF Packets	0
2	L2UCAST Packets	0
1	L2BCASTPackets	0
25		

Dell#

Example

```
param1=0(0x00)},
action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
meter=NULL,
counter={idx=1, mode=0x01, entries=1}

##### FP Entry for redirecting LACP traffic to CPU Port
```



```
#####
EID 2045: gid=1,
slice=15, slice_idx=0x02, prio=0x7fd, flags=0x82, Installed
tcam: color_indep=0, higig=0, higig_mask=0,
KEY=0x00000000 00000000 00000000 0180c200 00020000 00000000 00000000
, FPF4=0x00
MASK=0x00000000 00000000 00000000 ffffffff ffff0000 00000000 00000000
,
0x00
action={act=Drop, param0=0(0x00), param1=0(0x00)},
action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
meter=NULL,
counter={idx=2, mode=0x01, entries=1}

##### FP Entry for redirecting GVRP traffic to RSM #####
EID 2044: gid=1,
slice=15, slice_idx=0x03, prio=0x7fc, flags=0x82, Installed
tcam: color_indep=0, higig=0, higig_mask=0,
KEY=0x00000000 00000000 00000000 0180c200 00210000 00000000 00000000
, FPF4=0x00
MASK=0x00000000 00000000 00000000 ffffffff ffff0000 00000000 00000000
,
0x00
action={act=Drop, param0=0(0x00), param1=0(0x00)},
action={act=CosQCpuNew, param0=7(0x07), param1=0(0x00)},
action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
meter=NULL,
counter={idx=3, mode=0x01, entries=1}

##### FP Entry for redirecting ARP Replies to RSM #####
EID 2043: gid=1,
slice=15, slice_idx=0x04, prio=0x7fb, flags=0x82, Installed
tcam: color_indep=0, higig=0, higig_mask=0,
KEY=0x00000000 00000000 00000000 00000000 00000000 00000806 00001600
, FPF4=0x00
MASK=0x00000000 00000000 00000000 00000000 00000000 0000ffff 00001600
,
0x00
action={act=Drop, param0=0(0x00), param1=0(0x00)},
action={act=CosQCpuNew, param0=6(0x06), param1=0(0x00)},
action={act=CopyToCpu, param0=0(0x00), param1=0(0x00)},
action={act=UpdateCounter, param0=1(0x01), param1=0(0x00)},
!----- output truncated -----!
```

show hardware vlan-counters

Display the hardware VLAN statistics.

Syntax `show hardware vlan-counters vlan-id`

Parameters

vlan-id Enter the interface VLAN number. The 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced this command.

Example

```
Dell#show hardware vlan-counters 1
Counters for vlanid: 1
-----
Total number of inpackets: 0
Total number of inbytes: 0
Total number of outpackets: 0
Total number of outbytes: 0
Dell#
```

Related Commands [clear hardware system-flow](#) — clears the statistics from selected hardware components.

show hardware stack-unit buffer-stats-snapshot

View the buffer statistics tracking resource information without polling details and historical snapshots. This command is supported on the S6000 platform.

Syntax `show hardware stack-unit stack-unit-number buffer-stats-snapshot unit number resource X`

Parameters	stack-unit <i>stack-unit-number</i>	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. The range is 0 to 11.
	buffer-stats-snapshot unit <i>number</i>	Display the historical snapshot of buffer statistical values unit Enter the keyword <i>unit</i> along with a port-pipe number, then the keyword <i>counters</i> to display the counters on the selected port-pipe. The range is 0 to 0.
	port	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

Command Modes EXEC
EXEC Privilege

Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	Version 9.3(0.0)	Introduced on the S6000 platform.



Usage Information

The following information is displayed depending on whether the historical snapshot of buffer statistics is needed for all ports, per-port per-queue, or a priority group.

- All – Displays all resources on ingress and egress for each of the port, queue.
- Port-Queue ucast/mcast – Displays the total unicast/multicast buffer usage on per-port per-queue basis. For CPU port, counters for queues 0 – 11 are displayed and no differentiation is made between unicast and multicast queues.
- Port- Priority-Group – Displays the shared space counters usage, head-room space counters per ingress port on per-priority- group granularity.

When the buffer-stats-snapshot is disabled, an informational message is displayed to this effect when you attempt to view the buffer statistics tracking resource information without polling details and historical snapshots.

Example

```
Dell#show hardware stack-unit 1 buffer-stats-snapshot unit 0 resource port 1 queue u
Stack-unit: 1 unit: 0 port: 1 (interface Fo 1/4)
```

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#show hardware stack-unit 1 buffer-stats-snapshot unit 0 resource port 5 queue a
Stack-unit 1 unit 0 port 5 (interface te 1/4/1)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
UCAST		5	4
UCAST		6	8
UCAST		11	1
MCAST		4	11

Only the queues for which the buffer cell consumption is not zero are displayed. If an egress buffer is not present on any o sample output is displayed:

```
Dell#show hardware stack-unit 1 buffer-stats-snapshot unit 0 resource port 5 queue a
Stack-unit 1 unit 0 port 5 (interface te 1/4/1)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS

-

```
Dell#show hardware stack-unit 1 buffer-stats-snapshot unit 0 resource port 5 prio-gr
Stack-unit 1 unit 0 port 5 (interface te 1/4/1)
```

PG#	SHARED CELLS	HEADROOM CELLS



6	1000	5
7	3	0

show hardware stack-unit buffer-stats-snapshot (Total Buffer Information)

View the buffer statistics tracking resource information depending on the type of buffer information, such as device-level details, port-level counters, queue-based snapshots, or priority group-level snapshot in the egress and ingress direction of traffic.

Syntax `show hardware stack-unit <id> buffer-stats-snapshot unit <id> resource x`

Parameters

stack-unit <i>stack-unit-number</i>	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. The unit ID range from 1 to 6.
buffer-stats-snapshot unit <i>number</i>	Display the historical snapshot of buffer statistical values unit Enter the keyword <code>unit</code> along with a port-pipe number. The range is from 0 to 0.
buffer-info	Buffer and traffic manager resources usage, where X can be one of the following: • All - Displays ingress and egress device, port, and queue snapshots • Interface all queue {all} - egress queue-level snapshot for both unicast and multicast packets • Interface all queue ucast {id all} - egress queue-level snapshot for unicast packets only • Interface all queue mcast {id all} - egress queue-level snapshot for multicast packets only • Interface all prio-group {id all} - ingress priority-group level snapshot

Command Modes EXEC
EXEC Privilege

Command History

Version	Description
9.8(0.0)	Added the keyword <code>interface all</code> .
9.7(0.0)	Introduced on the S6000-ON.
9.6(0.0)	Introduced on the S5000.
9.3(0.0)	Introduced on the S6000, S4810, and S4820T.

Usage Information

The following information is displayed based on the buffer-info type, such as device-level details, queue-based snapshots, or priority group-level snapshot in the egress and ingress direction of traffic:

- Device-ingress – Displays total buffer accounting usage for the unit.
- Device-egress – Display total buffer usage for the unit, total multicast buffer usage for the unit and also on per-service-pool basis. Counters will be displayed for the 2 service-pools – one for normal traffic and other for DCB traffic.



When the buffer-stats-snapshot is disabled, the following informational message is displayed when you run the show command: %Info: Buffer-stats-snapshot feature is disabled.

Example

```
Dell#show hardware stack-unit 1 buffer-stats-snapshot unit 3 resource
interface all queue mcast 3
Unit 1 unit: 3 port: 1 (interface Fo 1/144)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
MCAST		3	0

```
Unit 1 unit: 3 port: 5 (interface Fo 1/148)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
MCAST		3	0

```
Unit 1 unit: 3 port: 9 (interface Fo 1/152)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
MCAST		3	0

```
Unit 1 unit: 3 port: 13 (interface Fo 1/156)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
MCAST		3	0

```
Unit 1 unit: 3 port: 17 (interface Fo 1/160)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
MCAST		3	0

```
Unit 1 unit: 3 port: 21 (interface Fo 1/164)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
MCAST		3	0

```
Unit 1 unit: 3 port: 25 (interface Fo 1/168)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
MCAST		3	0

```
Unit 1 unit: 3 port: 29 (interface Fo 1/172)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
MCAST		3	0

```
Unit 1 unit: 3 port: 33 (interface Fo 1/176)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS
MCAST		3	0

```
Unit 1 unit: 3 port: 37 (interface Fo 1/180)
```

Q#	TYPE	Q#	TOTAL BUFFERED CELLS



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 operating system supports the basic DHCP commands on this platform.

This chapter contains the following sections:

- [Commands to Configure the System to be a DHCP Server](#)
- [Commands to Configure Secure DHCP](#)

Commands to Configure the System to be a DHCP Server

To configure the system to be a DHCP server, use the following commands.

clear ip dhcp

Reset the DHCP counters.

Syntax	<code>clear ip dhcp [binding {address} conflict server statistics]</code>	
Parameters	binding	Enter the keyword <code>binding</code> to delete all entries in the binding table.
	address	Enter the IP address to clear the binding entry for a single IP address.
	conflicts	Enter the keyword <code>conflicts</code> to delete all of the log entries created for IP address conflicts.
	server statistics	Enter the keywords <code>server statistics</code> to clear all the server counter information.
Defaults	none	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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-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 server

Display FTOS debugging messages for DHCP.

Syntax `debug ip dhcp server [events | packets]`

Parameters

events	Enter the keyword <code>events</code> to display the DHCP state changes.
packet	Enter the keyword <code>packet</code> to display packet transmission/reception.

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
9.7(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.

debug ipv6 dhcp

To enable debug logs for DHCPv6 relay agent transactions.

Syntax `debug ipv6 dhcp`
To disable the debug logs for dhcpv6 relay agent transactions, use the `debug ipv6 dhcp` command.

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
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.

default-router

Assign a default gateway to clients based on the address pool.

Syntax	<code>default-router address [address2...address8]</code>	
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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

disable

Disable the DHCP server.

Syntax	<code>disable</code> DHCP Server is disabled by default. To enable the system to be a DHCP server, use the <code>no disable</code> command.	
Defaults	Disabled	
Command Modes	CONFIGURATION 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
9.7(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.

dns-server

Assign a DNS server to clients based on address pool.

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
9.7(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.

domain-name

Assign a domain to clients based on the address pool.

Syntax `domain-name name`



Parameters	<i>name</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

excluded-address

Prevent the server from leasing an address or range of addresses in the pool.

Syntax	<code>excluded-address [<i>address</i> <i>low-address high-address</i>]</code>	
Parameters	<i>address</i>	Enter a single address to be excluded from the pool.
	<i>low-address</i>	Enter the lowest address in a range of addresses to be excluded from the pool.
	<i>high-address</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.



hardware-address

For manual configurations, specify the client hardware address.

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
9.7(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.

host

For manual (rather than automatic) configurations, assign a host to a single-address pool.

Syntax `host address`

Parameters

address/mask	Enter the host IP address and subnet mask.

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
9.7(0.0)	Introduced on the S6000-ON.
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-Series and S-Series.

lease

Specify a lease time for the addresses in a pool.

Syntax `lease {days [hours] [minutes] | infinite}`

Parameters	<i>days</i>	Enter the number of days of the lease. The range is from 0 to 31.
	<i>hours</i>	Enter the number of hours of the lease. The range is from 0 to 23.
	<i>minutes</i>	Enter the number of minutes of the lease. The range is from 0 to 59.
	<i>infinite</i>	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
9.7(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.

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.

Syntax `netbios-name-server address [address2...address8]`

Parameters	<i>address</i>	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
9.7(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.

netbios-node-type

Specify the NetBIOS node type for a Microsoft DHCP client. Dell Networking recommends specifying clients as `hybrid`.

Syntax `netbios-node-type type`

Parameters

type	Enter the NETBIOS node type: • Broadcast: Enter the keyword <code>b-node</code>. • Hybrid: Enter the keyword <code>h-node</code>. • Mixed: Enter the keyword <code>m-node</code>. • Peer-to-peer: Enter the keyword <code>p-node</code>.

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
9.7(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.



network

Specify the range of addresses in an address pool.

Syntax	<code>network network /prefix-length</code>	
Parameters	<i>network/prefix-length</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

pool

Create an address pool.

Syntax	<code>pool name</code>	
Parameters	<i>name</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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-Series and S-Series.

show ip dhcp binding

Display the DHCP binding table.

Syntax	<code>show ip dhcp binding</code>
Defaults	none
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

show ip dhcp configuration

Display the DHCP configuration.

Syntax	<code>show ip dhcp configuration [global pool <i>name</i>]</code>				
Parameters	<table> <tr> <td>pool <i>name</i></td><td>Display the configuration for a DHCP pool.</td></tr> <tr> <td>global</td><td>Display the DHCP configuration for the entire system.</td></tr> </table>	pool <i>name</i>	Display the configuration for a DHCP pool.	global	Display the DHCP configuration for the entire system.
pool <i>name</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .				

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.
9.0.2.0	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.

show ip dhcp conflict

Display the address conflict log.

Syntax `show ip dhcp conflict address`

Parameters

<i>address</i>	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
9.7(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.

show ip dhcp server

Display the DHCP server statistics.

Syntax `show ip dhcp server statistics`

Defaults none

Command Modes EXEC Privilege

Command History

Version	Description
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 the C-Series and S-Series.

Commands to Configure Secure DHCP

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.

arp inspection

Enable dynamic arp inspection (DAI) on a VLAN.

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
9.7(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.
8.3.1.0	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 as trusted so that ARP frames are not validated against the binding table.

Syntax `arp inspection-trust`



Defaults	Disabled
Command Modes	· INTERFACE · INTERFACE PORT-CHANNEL
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
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.

Syntax `clear ip dhcp snooping {binding | source-address-validation discard-counters [interface interface]}`

Parameters	binding	Clears the binding table.
	source-address-validation discard-counters	Clears discard counters from all the interfaces configured with IP Source Guard.
	interface <i>interface</i>	(OPTIONAL) Specifies an interface to clear the discard counters.

Enter any of the following keywords and slot/port[/subport] or number 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.

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
9.7(0.0)	Introduced on the S6000-ON.
9.6(0.0)	Added the keywords <code>discard-counters</code> , <code>interface</code> , and the variable <code>interface</code> on the S4810, S4820T, S5000, S6000, Z9000, 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.
8.3.1.0	Introduced on the E-Series.
8.2.1.0	Introduced on the C-Series and S-Series.

Example The following example shows how to clear the discard counters globally:

```
Dell> clear ip dhcp snooping source-address-validation discard-counters
```

The following example shows how to clear the discard counters on an interface:

```
Dell> clear ip dhcp snooping source-address-validation discard-counters  
interface TenGigE 1/10/1
```

The following example shows how to clear the discard counters on a port channel interface:

```
Dell> clear ip dhcp snooping source-address-validation discard-counters  
interface portchannel 1
```

Related Commands [show ip dhcp snooping](#) — displays the contents of the DHCP binding table.

clear ipv6 dhcp snooping binding

Clear all the DHCPv6 snooping binding database entries.

Syntax `clear ipv6 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
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.

Example

```
Dell# clear ipv6 dhcp snooping?  
binding Clear the snooping binding database
```

ip dhcp relay

Enable Option 82.

Syntax	<code>ip dhcp relay information-option [remote-id trust-downstream]</code>	
Parameters	remote-id	Configure the system to enable the remote-id string in option-82.
	trust-downstream	Configure the system to trust Option 82 when it is received from the previous-hop router.
Defaults	Disabled	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.2(0.2)	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
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

Enable DHCP snooping globally.

Syntax	<code>[no] ip dhcp snooping</code>
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
9.2.(0.0)	Introduced on the S4810 and S4820T.
8.3.11.1	Introduced on the Z9000.



Version	Description
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.

Introduced in Dell Networking OS version 7.8.1.0, DHCP snooping was available for Layer 3 only and dependent on DHCP Relay Agent (`ip helper-address`). Dell Networking OS version 8.2.1.0 extends DHCP Snooping to Layer 2. You do not have to enable relay agent to snoop on Layer 2 interfaces.

ipv6 dhcp snooping

Enable DHCPv6 snooping globally for ipv6.

Syntax `[no] ipv6 dhcp snooping`
To disable the snooping globally, use the `no ipv6 dhcp 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
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.

ipv6 dhcp snooping vlan

Enable ipv6 DHCP Snooping on VLAN or range of VLANs.

Syntax `[no] ip dhcp snooping vlan vlan-id`
To disable the ipv6 dhcp snooping on VLAN basis or range of VLAN, use the `no ipv6 dhcp snooping vlan <vlan-id>` command.

Parameters *vlan-id* Enter the name of a VLAN id or list of the VLANs 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
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.

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 type slot/port[/subport] lease number`

Parameters	mac address	Enter the keyword <code>mac</code> then the MAC address of the host to which the server is leasing the IP address.
	vlan-id vlan-id	Enter the keywords <code>vlan-id</code> then the VLAN to which the host belongs. The range is from 2 to 4094.
	ip ip-address	Enter the keyword <code>ip</code> then the IP address that the server is leasing.
	interface type	Enter the keyword <code>interface</code> then the type of interface to which the host is connected: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
	slot/port[/subport]	Enter the slot and port number of the interface. Enter the subport number if a 40G port is fanned-out into 10G ports.
	lease time	Enter the keyword <code>lease</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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.
8.3.7.0	Introduced on the S4810.



Version	Description
8.3.1.0	Introduced on the E-Series.
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.

IPv6 DHCP Snooping Binding

Create a static DHCP snooping binding entry in the snooping database.

Syntax `[no] ipv6 dhcp snooping binding mac address vlan-id vlan-id ipv6 ipv6-address interface interface-type | interface-number lease value`
 To delete the DHCP snooping binding entry from DHCP snooping database, use the `[no] ipv6 dhcp snooping binding mac address vlan-id vlan-id ipv6 ipv6-address interface interface-type | interface-number lease value` command.

Parameters	mac address	Enter the keyword <code>mac</code> then the MAC address of the host to which the server is leasing the IPv6 address.
	vlan-id	Enter the keywords <code>vlan-id</code> then the VLAN to which the host belongs. The range is from 2 to 4094.
	ipv6 ipv6-address	Enter the keyword <code>ipv6</code> then the IPv6 address that is leased to the client.
	interface type	Enter the keyword <code>interface</code> then the type of interface to which the host is connected: - For an 10/100 Ethernet interface, enter the keyword <code>fastethernet</code>. - For a Gigabit Ethernet interface, enter the keyword <code>gigabitethernet</code>. - For a Ten-Gigabit Ethernet interface, enter the keyword <code>tengigabitethernet</code>. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code>.
	interface number	Enter the number of the interface.
	lease value	Enter the keyword <code>lease</code> then the amount of time the IPv6 address are leased. The range is from 1 to 4294967295.

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
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.



ip dhcp snooping database

Delay writing the binding table for a specified time.

Syntax `ip dhcp snooping database write-delay minutes`

Parameters

<i>minutes</i>	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
9.7(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.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

ipv6 dhcp snooping database write-delay

To set time interval for storing the snooping binding entries in a file.

Syntax `[no] ipv6 dhcp snooping database write-delay value`

To disable the storing of snooping binding entries in a file, use the `no ipv6 dhcp snooping write-delay` command.

Parameters

<i>value</i>	The range is from 5 to 21600. The value of the minutes range is from 5 min. to 15 days.

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
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.

ip dhcp snooping database renew

Renew the binding table.

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
9.7(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.
8.3.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series.

ipv6 dhcp snooping database renew

To load the binding entries from the file to DHCPv6 snooping binding database.

Syntax `ipv6 dhcp snooping database renew`

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
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.



ip dhcp snooping trust

Configure an interface as trusted.

Syntax	<code>[no] ip dhcp snooping trust</code>
Defaults	Untrusted
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 the C-Series and S-Series.

ipv6 dhcp snooping trust

Configure an interface as trusted for DHCP snooping.

Syntax	<code>[no] ipv6 dhcp snooping trust</code> To disable dhcp snooping trusted capability on this interface, use the <code>no ipv6 dhcp snooping trust</code> command.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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

Version	Description
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.

ip dhcp source-address-validation

Enable the IP Source Guard.

Syntax	<code>[no] ip dhcp source-address-validation [ipmac] [vlan vlan-id]</code>
Parameters	ipmac Enable IP+MAC Source Address Validation.



vlan *vlan-id* (OPTIONAL) SAV validates the source IP address along with the source VLAN ID against the DHCP snooping binding table.

Defaults Disabled

Command Modes INTERFACE

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
9.7(0.0)	Introduced on the S6000-ON.
9.6(0.0)	Added the <code>vlan</code> keyword and the <code>vlan-id</code> variable . Introduced support for SAV on port channels interfaces.
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.
8.2.1.0	Added the keyword <code>ipmac</code> .
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 and SAV with VLAN option.

1. Use the `cam-acl 12acl` command from CONFIGURATION mode.
2. Save the running-config to the startup-config.
3. Reload the system.

ip dhcp relay information-option

Enable Option 82.

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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.4.(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 snooping verify mac-address

Validate a DHCP packet's source hardware address against the client hardware address field (CHADDR) in the payload.

Syntax	<code>[no] ip dhcp snooping verify mac-address</code>
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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
8.3.1.0	Introduced on the E-Series.
7.2.1.0	Introduced on the C-Series and S-Series.

ipv6 dhcp snooping verify mac-address

Syntax `[no] ipv6 dhcp snooping verify mac-address`
 To disable verify source mac-address against IPv6 DHCP packet MAC address, use the `no ipv6 dhcp snooping verify mac-address` 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
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.

ip helper-address

Configures the destination broadcast address or the host address for DHCP server requests.

Syntax `ip helper-address [vrf vrf-name] ip-address`
 To disable the destination broadcast address or the host address for DHCP server requests, use the `ip helper-address [vrf vrf-name] ip-address` command.

Parameters

vrf vrf-name	(Optional) Enter the keyword <code>vrf</code> and then the name of the VRF through which the host address can be reached.
ip-address	Enter an IP address through which the host address can be reached.

Default 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
Version 9.4.(0.0)	Introduced on the S-Series and Z-Series.



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-fo-1/12)#ip helper-address vrf jay 10.0.0.2`

ipv6 helper-address

Configures the ipv6 DHCP helper addresses without VRF.

Syntax `[no] ipv6 helper-address ipv6-address`

To delete the ipv6 helper address, use the `[no] ipv6 helper-address ipv6-address` command.

Parameters

ipv6-address	Enter the keyword <code>ipv6-address</code> 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, refer to the relevant *Dell 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 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.
Global          Global address space
```

show ip dhcp snooping

Display the contents of the DHCP binding table or display the interfaces configured with IP Source Guard.

Syntax `show ip dhcp snooping [binding | source-address-validation [discard-counters [interface interface]]]`

Parameters

binding	Display the binding table.
source-address-validation	Display the interfaces configured with IP Source Guard.
discard-counters	(OPTIONAL) Display the number of dropped packets.



interface interface (OPTIONAL) Specifies an interface to show the discard counters.

Enter any of the following keywords and slot/port[/subport] or number 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.

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
9.6(0.0)	Added the <code>discard-counters</code> , <code>interface</code> keywords, and the <code>interface</code> variable.
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 the C-Series and S-Series.

Example The following example displays the interfaces configured with IP Source Guard:

```
Dell> show ip dhcp snooping source-address-validation
ip sav access-list on TenGigabitEthernet 1/1/1
Total cam count 3
permit host 0.0.0.0 count (0 packets)
permit host 10.1.1.252 count (0 packets)
permit host 10.1.1.253 count (0 packets)
ipmac-vlan sav access-list on TenGigabitEthernet 1/1/2
Total cam count 4
permit host 0.0.0.0 host 00:00:00:00:00:00 count (0 packets)
permit vlan 10 host 10.1.1.1 host 00:00:00:aa:00:01 count (0 packets)
permit vlan 10 host 10.1.1.2 host 00:00:00:aa:00:02 count (0 packets)
permit vlan 20 host 10.2.2.1 host 00:00:00:aa:00:03 count (0 packets)
permit vlan 20 host 10.2.2.2 host 00:00:00:aa:00:04 count (0 packets)
```

The following example displays the port channel interfaces configured with IP Source Guard:

```
Dell> show ip dhcp snooping source-address-validation interface
portchannel 10
ipmac-vlan sav access-list on Port-channel 10 on stack-unit 1
Total cam count 5
```



```

permit host 0.0.0.0 host 00:00:00:00:00:00 count (0 packets)
permit vlan 10 host 1.1.1.1 host 00:00:00:00:01:01 count (0 packets)
permit vlan 10 host 1.1.1.2 host 00:00:00:00:01:02 count (0 packets)
permit vlan 10 host 1.1.1.3 host 00:00:00:00:01:03 count (0 packets)
ipmac-vlan sav access-list on Port-channel 10 on stack-unit 2
Total cam count 5
permit host 0.0.0.0 host 00:00:00:00:00:00 count (0 packets)
permit vlan 10 host 1.1.1.1 host 00:00:00:00:01:01 count (0 packets)
permit vlan 10 host 1.1.1.2 host 00:00:00:00:01:02 count (0 packets)
permit vlan 10 host 1.1.1.3 host 00:00:00:00:01:03 count (0 packets)
ipmac-vlan sav access-list on Port-channel 10 on stack-unit 3
Total cam count 5
permit host 0.0.0.0 host 00:00:00:00:00:00 count (0 packets)
permit vlan 10 host 1.1.1.1 host 00:00:00:00:01:01 count (0 packets)
permit vlan 10 host 1.1.1.2 host 00:00:00:00:01:02 count (0 packets)
permit vlan 10 host 1.1.1.3 host 00:00:00:00:01:03 count (0 packets)

```



NOTE: The output for port-channel interfaces does not display the physical interface.

The following example displays the SAV discard counters on all interfaces:

```

Dell> show ip dhcp snooping source-address-validation discard-counters
deny access-list on TenGigabitEthernet 1/1/1
Total cam count 1
deny count (0 packets)
deny access-list on TenGigabitEthernet 1/1/2
Total cam count 2
deny vlan 10 count (0 packets)
deny vlan 20 count (0 packets)

```

The following example displays the SAV discard counters on a particular interface:

```

Dell> show ip dhcp snooping source-address-validation discard-counters
interface TenGigabitEthernet 1/1/1
deny access-list on TenGigabitEthernet 1/1/1
Total cam count 2
deny vlan 10 count (0 packets)
deny vlan 20 count (0 packets)

```

The following example displays the SAV discard counters on a port channel interface:

```

Dell> show ip dhcp snooping source-address-validation discard-counters
interface portchannel 10
deny access-list on Port-channel 10 on stack-unit 1
Total cam count 1
deny vlan 10 count (0 packets)
deny access-list on Port-channel 10 on stack-unit 2
Total cam count 1
deny vlan 10 count (0 packets)
deny access-list on Port-channel 10 on stack-unit 3
Total cam count 1
deny vlan 10 count (0 packets)

```



NOTE: The output for port-channel interfaces does not display the physical interface. If the LAG member interfaces belong to different stack-units, the counters are displayed per stack-unit for that port channel.

show ipv6 dhcp snooping

Display the DHCPv6 snooping binding database.

Syntax show ipv6 dhcp snooping

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
9.7(0.0)	Introduced on the S4810, S4820T, S6000 and Z-Series.

Example

```
Dell#show ipv6 dhcp snooping
IPv6 DHCP Snooping                : Enabled.
IPv6 DHCP Snooping Mac Verification : Disabled.

Database write-delay (In minutes)  : 5

DHCP packets information
Snooping packets                  : 0
Snooping packets processed on L2 vlans : 0

DHCP Binding File Details
Invalid File                      : 0
Invalid Binding Entry             : 0
Binding Entry lease expired       : 0

Dell#
```

Commands to Configure DNS

To configure the Domain Names Systems (DNS) on the system, use the following commands:

ip name-server

Configures the name server IP addresses for VRF. Using this command, you can configure up to a maximum of six IP addresses per VRF.

Syntax

```
ip name-server [vrf vrf-name] ip-address [ip-address2] [ip-address3] [ip-
address4] [ip-address5] [ip-address6]
```

To undo the name server ip address configuration for VRF, use the `no ip name-server [vrf vrf-name] ip-address` command.

Parameters

vrf vrf-name (Optional) Enter the key word `vrf` and then the name of the VRF to configure the name server IP addresses for that VRF.

ip-address [ip-address2] [ip-address3] [ip-address4] [ip-address5] [ip-address6] Enter the IP address of the name server in dotted decimal format.



NOTE: Use the additional *ip-address* parameters (*ip-address2* to *ip-address6*) in a sequential order to specify up to a maximum of six IP addresses per 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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S-Series and Z-Series.

Usage Information Use this command to associate name server IP addresses to a specific VRF.

Example

- `Dell(conf)#ip name-server vrf jay 2.2.2.2`
- `Dell(conf)#ip name-server vrf jay 2.2.2.2 3.3.3.3 4.4.4.4 5.5.5.5 6.6.6.6 7.7.7.7`

ip domain-name

Configures the default domain corresponding to a specific VRF. This domain is appended to the in complete DNS requests corresponding to the specified VRF.

Syntax `ip domain-name [vrf vrf-name] name`

To undo the domain name configuration corresponding to a specific VRF, use the `no ip domain-name [vrf vrf-name] name` command.

Parameters

vrf vrf-name	(Optional) Enter the key word <code>vrf</code> and then the name of the VRF to configure the domain corresponding to that VRF.
name	Enter the name of the domain to be appended to the in complete DNS requests corresponding to the specified VRF.

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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S-Series and Z-Series.

Usage Information Use this command to configure a domain name corresponding to a VRF. This domain is appended to the in complete DNS requests corresponding to the specified VRF.

Example `Dell(conf)#ip domain-name vrf jay dell.com`



ip domain-list

Adds a domain name to the DNS list. This domain name is appended to incomplete host names in DNS requests corresponding to a specific VRF.

Syntax `ip domain-list [vrf vrf-name] name`

To remove a domain name from DNS list, use the `no ip domain-list [vrf vrf-name] name` command.

Parameters

vrf *vrf-name* (Optional) Enter the key word `vrf` and then the name of the VRF to add a domain name to the DNS list corresponding to that VRF.

name Enter the name of the domain to be appended to the DNS list corresponding to the VRE.

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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S-Series and Z-Series.

Usage Information	Use this command to add domain names to the DNS lists corresponding to a specific VRF. You can add up to a maximum of six domain names to the DNS list corresponding to a VRF. This domain is used to complete the unqualified host names.

```
Example      Dell(conf)#ip domain-list vrf jay dell.com
             Dell(conf)#ip domain-list vrf jay force10.com
```

ip host

Configures a mapping between the host name server and the IP address for a specific VRF. This mapping information is used by the name-to-IP address table to resolve host names.

Syntax `ip host [vrf vrf-name] name ip-address`

To undo the host name server to IP address mapping for VRFs, use the `no ip host [vrf vrf-name] name ip-address` command.

Parameters

vrf *vrf-name* (Optional) Enter the key word `vrf` and then the name of the VRF to configure the name server to IP address mapping for that VRF.

name Enter the name of the host to be associated with an IP address.



ip-address Enter the IP address of the name server in dotted decimal format.

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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S-Series and Z-Series.

Usage Information Use this command to create a mapping between a host name server and its IP addresses for a specific VRF.

Example `Dell(conf)#ip host vrf jay dell 1.1.1.1`

clear host

Removes one or all dynamically learned host table entries for a specific VRF.

Syntax `clear host [vrf vrf-name] [* | host-name]`

Parameters

<i>vrf vrf-name</i>	(Optional) Enter the key word <code>vrf</code> and then the name of the VRF to delete dynamically learned host table entries corresponding to that VRF.
<i>host-name</i>	Enter the name of the host corresponding to which you want to delete the dynamically learnt host table entries.
<i>*</i>	Enter <code>*</code> to delete all host table entries.

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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S-Series and Z-Series.

Usage Information Use this command to delete one or all dynamically learned host table entries corresponding to a specific VRF.

Example `Dell#clear host vrf jay dell`
`Dell#clear host vrf jay *`



Equal Cost Multi-Path (ECMP)

Equal cost multi-path (ECMP) is supported on the Dell Networking OS.

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.

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

<i>ecmp-group ID</i>	Enter the identifier number for the ECMP group. The range is from 2 to 64.
<i>interface</i>	Enter the following keywords and slot/port[/subport] to add the interface to the ECMP group: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a LAG interface, enter the keywords <code>port-channel</code> 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, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.



Version	Description
8.3.19.0	Introduced on the S4820T.
8.3.10.0	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 port-channel configuration using the CONFIGURATION ECMP-GROUP command mode.

hash-algorithm

Changes the hash algorithm used to distribute traffic flows across a Port Channel. The ECMP and LAG options are supported on the Z-Series.

Syntax

```
hash-algorithm {algorithm-number | {ecmp {crc16 | crc16cc | crc32MSB |
crc32LSB | crc-upper | dest-ip | lsb | xor1 | xor2 | xor4 | xor8 | xor16}
[number] hg {crc16 | crc16cc | crc32MSB | crc32LSB | xor1 | xor2 | xor4 |
xor8 | xor16} stack-unit stack-unit-number | port-set port-pipe | hg-seed
seed-value stack-unit | lag {checksum | crc | xor} [number] nh-ecmp
{checksum | crc | xor}[number] stack-unit number ip-sa-mask value ip-da-
mask value | seed seed-value }
```

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 stack-unit, use the `no hash-algorithm linecard number` command.

Parameters

algorithm-number	Enter the algorithm number. The range is from 0 to 47.
ecmp <i>algorithm-number</i> <i>algorithm-number</i>	TeraScale and ExaScale Only: Enter the keyword <code>ecmp</code> then one of the following options:
<i>algorithm-number</i> <i>algorithm-number</i>	<i>algorithm-number</i>: Use CRC16_BISYNC — 16 bit CRC16-bisync polynomial (default) <i>algorithm-number</i>: Use CRC16_CCITT — 16 bit CRC16 using CRC16-CCITT polynomial <i>algorithm-number</i>: Use CRC32_UPPER — MSB 16 bits of computed CRC32 <i>algorithm-number</i>: Use CRC32_LOWER — LSB 16 bits of computed CRC32 <i>algorithm-number</i>: Uses the upper 32 bits of the key for the hash computation <i>algorithm-number</i>: Uses the destination IP for ECMP hashing <i>algorithm-number</i>: Returns the LSB of the key as the hash <i>algorithm-number</i>: Use CRC16_BISYNC_AND_XOR1 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor1 <i>algorithm-number</i>: Use CRC16_BISYNC_AND_XOR2 — Upper 8 bits of CRC16-BISYNC and lower 8 bits of xor2 <i>algorithm-number</i>: 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*} **stack-unit** *stack-unit-number* | **port-set** *port-pipe*

Z-Series only: 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

Enter the keywords **stack-unit**, then a stack-unit number, to specify a stack-unit.

Enter the keywords **port-set** *port-pipe* then the port pipe number. The range is from 0 to 5.

hg-seed *seed-value* **stack-unit**

Z-Series only: Enter the keywords **hg-seed** then the hash algorithm seed value. The range is from 0 to 2147483646.

Enter the keywords **stack-unit** then the stack unit number.

Enter the keywords **port-set** then the stack-unit port-pipe number.

lag *hash algorithm*

Z-Series only: Enter the keywords **hg-seed** . The range is from 0 to 47.

nh-ecmp *hashalgorithm* *value*

(OPTIONAL) Enter the keyword **nh-ecmp** followed by the ECMP hash algorithm value.

stack-unit *number*

(OPTIONAL) : Enter the keyword **stack—unit** followed by the stack—unit slot number.

ip-sa-mask *value*

(OPTIONAL) Enter the keyword **ip-sa-mask** followed by the ECMP/LAG hash mask value. The range is from 0 to FF.

ip-da-mask *value*

(OPTIONAL) Enter the keyword **ip-da-mask** followed by the ECMP/LAG hash mask value. The range is from 0 to FF.

Defaults IPSA and IPDA mask value is **FF** for the stack-unit.

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Introduced on the S4810.
8.1.1.0	Introduced on the E-Series ExaScale.
7.8.1.0	Added the <code>nh-ecmp</code> option.
7.7.1.1	Added the <code>nh-ecmp</code> option.

Usage Information

To ensure that CRC is not used for LAG, set the default hash-algorithm method on ExaScale systems. For example, `hash-algorithm ecmp xor lag checksum nh-ecmp checksum`.

The hash value calculated with the `hash-algorithm` command is unique to the entire chassis. The hash algorithm command with the `stack—unit` option changes the hash for a particular stack—unit by applying the mask specified in the IPSA and IPDA fields.

The `stack-unit` option is applicable with the `lag-hash-align` microcode only. Any other microcode returns an error message as follows:

- `Dell(conf)#hash-algorithm linecard 5 ip-sa-mask ff ip-da-mask ff`
- `% Error: This command is not supported in the current microcode configuration`

In addition, the `linecard number ip-sa-mask value ip-da-mask value` option has the following behavior to maintain bi-directionality:

- 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, Dell Networking OS maintains bi-directionality with masks set to `XX 00` for stack-unit 1 and `00 XX` for stack-unit 2 (`ip-sa-mask` and `ip-da-mask`). The mask value must be the same for both stack-units when using multiple stack-units as ingress (where `XX` is any value from `00` to `FF` for both stack-units). For example, assume that traffic is flowing between linecard 1 and linecard 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.



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.

Syntax	<code>ip ecmp-group {maximum-paths {number} {path-fallback}</code>	
	To negate a command, use the <code>no ip ecmp-group maximum-paths {number}</code> command.	
Parameters	maximum-paths	Specify the maximum number of ECMP for a route. The range is 2 to 64.
	path-fallback	Use the keywords <code>path-fallback</code> 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
	9.7(0.0)	Introduced on the S6000-ON.
	9.0.2.0	Introduced on the S6000.
	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 (<code>write-mem</code>) then reload the system for the new settings to take effect.	
Related Commands	show ip cam stack-unit – Display content-addressable memory (CAM) entries for an S-Series switch.	

ip ecmp weighted

Enables weighted ECMP calculations.

Syntax	<code>ip ecmp weighted</code>	
	To disable weighted ECMP calculations, enter the <code>no ip ecmp weighted</code> command.	
Defaults	N/A	
Command Modes	CONFIGURATION	
Command History	Version	Description
	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.

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

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.



link-bundle-monitor enable

Provides a mechanism to enable monitoring of traffic distribution on an ECMP link bundle.

Syntax `link-bundle-monitor enable`
To exit from ECMP group 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, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
9.0.0.0	Introduced on the Z9000.
8.3.19.0	Introduced on the S4820T.
8.3.10.0	Introduced on the S4810.



Flex Hash and Optimized Boot-Up

This chapter describes the Flex Hash and fast-boot enhancements.

load-balance ingress-port enable

Enable the Flex hash functionality. This utility is supported on the platform.

Syntax	<code>load-balance ingress-port enable</code> To disable the Flex hash capability, use the no version of this command.
Default	None
Command Modes	CONFIGURATION mode
Command History	Version 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 <code>show ip flow</code>. As a result, when load balancing of RRoCE packets using Flex hash is enabled, the <code>show ip flow</code> command is not functional. Similarly, when <code>show ip flow</code> 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	<code>Dell#load-balance ingress-port enable</code>

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	<code>load-balance flexhash ipv4/ipv6 ip-proto <protocol number> <description string> offset1 <offset1 value> [offset2 <offset2 value>]</code> To disable the Flex hash settings, use the <code>no load-balance flexhash ipv4/ipv6 ip-proto protocol number</code> 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.
	<i>protocol number</i>	Represents the Outer IPv4 protocol field in case of IPv4 packets, and the Outer IPv6 next header field in case of IPv6 packets. The <code>ipv4/ipv6</code> 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	Version 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	<pre>Dell(conf)# load-balance flexhash ipv4 ip-proto 1 desc offset1 1 offset2 2</pre>	



reload-type fastboot

Restart the system with optimized booting-time functionality enabled. When you restart the device in fast boot mode, traffic disruption is reduced significantly and the system operations to service the data traffic are restored in a seamless way.

C9000 Series

Syntax `reload-type fastboot`

Parameters

fastboot	Enable the system to restart the next time with the optimized booting-time capability

Defaults By default, the device reloads in Jumpstart or BMP mode.

Command Modes GLOBAL CONFIGURATION

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.x.x.x	Introduced on the C9000.
9.3(0.0)	Added support for the <code>fastboot</code> parameter for S6000 platform.

Usage Information You can configure an optimization technique to reduce the booting time of an S6000 Switch. This mechanism is also called fast boot. With the reduced time that is taken to reboot the switch, upon a manually-initiated reload or an expected restart of the device, the disruption in traffic that is serviced by the switch is minimized. Traffic outage is lowered considerably (reduced to approximately 25 seconds in certain network deployments) when you enable this optimization method for booting of the device. By reducing the duration of traffic loss, subscriber sessions are processed and preserved in an effective and seamless way.

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.x.x.x	Introduced on the C9000.



Version	Description
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.

encapsulation dot1q

Configures lite-subinterfaces.

C9000 Series

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	Description
	9.x.x.x	Introduced on the C9000.
	9.3.0.0	Introduced on the S6000.

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 .



FIP Snooping

To enable the FCoE Transit feature and configure FIP snooping, use the following Dell Networking Operating System commands on the 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.

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.

Syntax	<code>clear fip-snooping database interface vlan {vlan-id} enode {enode-mac-address} fcf {fcf-mac-address} session {session-mac-address}</code>	
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
9.7(0.0)	Introduced on the Z9500 and S6000-ON.
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.

Syntax

```
clear fip-snooping statistics [interface vlan vlan-id | interface
fortyGigEport-type port/slot[/subport] | interface port-channel port-
channel-number]
```

Parameters

<i>vlan-id</i>	Enter the VLAN ID of the FIP packet statistics to be cleared.
<i>port-type port/slot</i>	Enter the port-type and slot number of the FIP packet statistics to be cleared. Enter the subport number if a 40G port is fanned-out into 10G ports.
<i>port-channel-number</i>	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
9.7(0.0)	Introduced on the Z9500 and S6000-ON.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

debug fip snooping

Enable debugging on FIP snooping.

Syntax

```
debug fip-snooping [all | acl | error | ifm | info | ipc | tx]
```

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.

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
9.7(0.0)	Introduced on the Z9500 and S6000-ON.
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.

Syntax `debug fip-snooping rx packet-type [all | discovery | virtual-link-instantiation | virtual-link-maintenance | vlan-discovery] [interface]`

Parameters

packet-type	Enter the keyword <code>packet-type</code> and then the option type on which to enable debugging. The options are: • <code>all</code> — Enter the keyword <code>all</code> to enable debugging on all the options. • <code>discovery</code> — Enter the keyword <code>discovery</code> to enable debugging on FCF advertisements and ENode solicitation. • <code>virtual-link-instantiation</code> — Enter the keywords <code>virtual-link-instantiation</code> to enable debugging on FLOGI, FDISC, and FLOGO packets. • <code>virtual-link-maintenance</code> — Enter the keywords <code>virtual-link-maintenance</code> to enable debugging on FIP clear virtual link frames and keepalives. • <code>vlan-discovery</code> — Enter the keywords <code>vlan-discovery</code> to enable debugging on VLAN requests and notifications.
interface	Enter the following keywords and slot/port[/subport] or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> then a 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 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 Z9500 and S6000-ON.
9.2(0.2)	Introduced on the S4810 and S4820T. Added the receive parameters <code>packet-type</code> and <code>interfaces</code> and their options.

feature fip-snooping

Enable FCoE transit and FIP snooping on a switch.

Syntax	<pre>feature fip-snooping</pre> To disable the FCoE transit feature, use the <code>no feature fip-snooping</code> command.
Defaults	Disabled
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. 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.
9.7(0.0)	Introduced on the Z9500.
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.

Syntax	<pre>fip-snooping enable</pre> To disable the FIP snooping feature on all or a specified VLAN, use the <code>no fip-snooping enable</code> 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the Z9500 and S6000-ON.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.7(0.0)	Introduced on the Z9500 and S6000-ON.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.
Version	Description								
9.7(0.0)	Introduced on the Z9500 and S6000-ON.								
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 four. The maximum number of FIP snooping sessions supported per ENode server is 16.								

fip-snooping fc-map

Configure the FC-MAP value FIP snooping uses on all VLANs.

Syntax	<pre>fip-snooping fc-map fc-map-value</pre> To return the configured FM-MAP value to the default value, use the <code>no fip-snooping fc-map</code> command.								
Parameters	<table> <tr> <td><i>fc-map-value</i></td><td>Enter the FC-MAP value FIP snooping uses. The range is from 0EFC00 to 0EFCFF.</td></tr> </table>	<i>fc-map-value</i>	Enter the FC-MAP value FIP snooping uses. The range is from 0EFC00 to 0EFCFF.						
<i>fc-map-value</i>	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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the Z9500 and S6000-ON.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> </table>	Version	Description	9.7(0.0)	Introduced on the Z9500 and S6000-ON.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.
Version	Description								
9.7(0.0)	Introduced on the Z9500 and S6000-ON.								
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.

Syntax	<code>fip-snooping max-sessions-per-enode-mac max-sessions-value</code> To return the configured maximum sessions to the default value, use the <code>no fip-snooping max-sessions-per-enode-mac</code> command.						
Parameters	<code>max-sessions-value</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the Z9500 and S6000-ON.</td></tr><tr><td>9.2(0.2)</td><td>Introduced on the S4810 and S4820T.</td></tr></table>	Version	Description	9.7(0.0)	Introduced on the Z9500 and S6000-ON.	9.2(0.2)	Introduced on the S4810 and S4820T.
Version	Description						
9.7(0.0)	Introduced on the Z9500 and S6000-ON.						
9.2(0.2)	Introduced on the S4810 and S4820T.						

fip-snooping port-mode fcf

Configure the port for bridge-to-FCF links.

Syntax	<code>fip-snooping port-mode fcf</code> To disable the bridge-to-FCF link on a port, use the <code>no fip-snooping port-mode fcf</code> command.								
Command Modes	INTERFACE								
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the Z9500 and S6000-ON.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr></table>	Version	Description	9.7(0.0)	Introduced on the Z9500 and S6000-ON.	8.3.19.0	Introduced on the S4820T.	8.3.12.0	Introduced on the S4810.
Version	Description								
9.7(0.0)	Introduced on the Z9500 and S6000-ON.								
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 four.								



fip-snooping port-mode fcoe-trusted

Configure the port for bridge-to-bridge links.

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
9.7(0.0)	This command is deprecated.
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



NOTE: This command is deprecated from the Dell Networking OS.

show fip-snooping config

Display the FIP snooping status and configured FC-MAP values.

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
9.7(0.0)	Introduced on the Z9500 and S6000-ON.
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.

Syntax

```
show fip-snooping enode [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
9.7(0.0)	Introduced on the Z9500 and S6000-ON.
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 1/11/1 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.

Syntax `show fip-snooping fcf [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, refer to the relevant *Dell 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 Z9500 and S6000-ON.
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 statistics

Display statistics on the FIP packets snooped on all interfaces, including VLANs, physical ports, and port channels.

Syntax `show fip-snooping statistics [interface vlan vlan-id | interface port-type port/slot[/subport] | interface port-channel port-channel-number]`

Parameters

<i>vlan-id</i>	Enter the VLAN ID of the FIP packet statistics displays.
<i>port-type</i> <i>port/slot</i> [/ <i>subport</i>]	Enter the port-type and slot number of the FIP packet statistics displays. Enter the subport number if a 40G port is fanned-out into 10G ports.
<i>port-channel-number</i>	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
9.7(0.0)	Introduced on the Z9500 and S6000-ON.
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.



Field	Description
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 1/11/1
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.

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
9.7(0.0)	Introduced on the Z9500 and S6000-ON.
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.

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
9.7(0.0)	Introduced on the Z9500 and S6000-ON.
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
```



show fips status

Display the FIPs status on the platform.

Syntax `show fips status`

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
9.7(0.0)	Introduced on the S6000-ON.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.



Force10 Resilient Ring Protocol (FRRP)

Force10 resilient ring protocol (FRRP) is supported on Dell Networking OS.

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.

clear frrp

Clear the FRRP statistics counters.

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
9.7(0.0)	Introduced on the S6000–ON.
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-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. Dell Networking OS 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.

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 <code>event</code> to display debug information related to ring protocol transitions.
	packet	Enter the keyword <code>packet</code> to display brief debug information related to control packets.
	detail	Enter the keyword <code>detail</code> 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 <i>number</i>	Enter the keyword <code>count</code> then the number of debug outputs. The range is from 1 to 65534.

Defaults Disabled.



Command Modes	CONFIGURATION (conf-frmp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
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.

Syntax	<code>description <i>Word</i></code> To remove the ring description, use the <code>no description [<i>Word</i>]</code> command.

Parameters	Word Enter a description of the ring. Maximum: 255 characters.

Defaults	none

Command Modes	CONFIGURATION (conf-frmp)

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

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.
9.0.2.0	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
8.2.1.0	Introduced on the C-Series.
7.4.1.0	Introduced.

disable

Disable the resilient ring protocol.

Syntax	<pre>disable</pre> To enable the Resilient Ring Protocol, use the <code>no disable</code> command.
Defaults	Disabled
Command Modes	CONFIGURATION (conf-frmp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. 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.
9.0.2.0	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.
7.4.1.0	Introduced.

interface

Configure the primary, secondary, and control-vlan interfaces.

Syntax	<pre>interface {primary interface secondary interface control-vlan vlan-id}</pre> To return to the default, use the <code>no interface {primary interface secondary interface control-vlan vlan-id}</code> command.



Parameters

primary interface	Enter the keyword <code>primary</code> to configure the primary interface then one of the following interfaces and slot/port[/subport] information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.
secondary interface	Enter the keyword <code>secondary</code> to configure the secondary interface then one of the following interfaces and slot/port[/subport] information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> then a number.
control-vlan <i>vlan-id</i>	Enter the keyword <code>control-vlan</code> 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
9.7(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.
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.

Syntax	<code>member-vlan {vlan-range}</code> To return to the default, use the <code>no member-vlan [vlan-range]</code> command.	
Parameters	<i>vlan-range</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	Introduced on the S6000.
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.

Syntax	<code>mode {master transit}</code> To reset the mode, use the <code>no mode {master transit}</code> command.	
Parameters	<i>master</i>	Enter the keyword <code>master</code> to set the Ring node to Master mode.
	<i>transit</i>	Enter the keyword <code>transit</code> 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
9.7(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.
74.1.0	Introduced.

protocol frrp

Enter the Resilient Ring Protocol and designate a ring identification.

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
9.7(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.
74.1.0	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.

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 <code>summary</code> 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
9.7(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.
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. Dell Networking OS 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

Usage Information Executing this command without the optional `ring-id` command clears the statistics counters on all the available rings. Dell Networking OS requires a command line confirmation before the command is executed. 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 1/16/1 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.

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 <i>milliseconds</i>	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 <i>milliseconds</i>	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
9.7(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.
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.



GARP VLAN Registration (GVRP)

The Dell Networking operating system supports the basic GVRP commands on the Dell Networking OS.

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.



clear gvrp statistics

Clear GVRP statistics on an interface.

Syntax `clear gvrp statistics interface interface`

Parameters

interface *interface*

Enter the following keywords and slot/port[/subport] or number 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.

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
9.7(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 C-Series, E-Series, and S-Series

Related Commands [show gvrp statistics](#) — displays the GVRP statistics.

debug gvrp

Enable debugging on GVRP.

Syntax `debug gvrp {config | events | pdu}`

To disable debugging, use the `no debug gvrp {config | events | pdu}` command.

Parameters

config	Enter the keyword <code>config</code> to enable debugging on the GVRP configuration.
event	Enter the keyword <code>event</code> to enable debugging on the JOIN/LEAVE events.
pdu	Enter the keyword <code>pdu</code> then one of the following Interface keywords and slot/port[/subport] or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.

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
9.7(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 C-Series, E-Series, and S-Series

disable

Globally disable GVRP.

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
9.7(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 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.

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 <code>join</code> 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 <code>leave</code> 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 <code>leave-all</code> 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
9.7(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 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.

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
9.7(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.
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.

Syntax `gvrp registration {fixed | normal | forbidden}`
To return to the default, use the `gvrp register normal` command.

Parameters	fixed	Enter the keyword <code>fixed</code> then the VLAN range in a comma-separated VLAN ID set.
	normal	Enter the keyword <code>normal</code> then the VLAN range in a comma-separated VLAN ID set. This setting is the default.
	forbidden	Enter the keyword <code>forbidden</code> 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
9.7(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 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)#.

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
9.7(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 C-Series, E-Series, and S-Series

Related Commands [disable](#) — globally disables GVRP.



show config

Display the global GVRP configuration.

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
9.7(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 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.

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
9.7(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.
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.

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[/subport] or number 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.

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
9.7(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 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 3/1/1            Disabled          No
Te 3/1/2            Enabled           No
Te 3/1/3            Disabled          No
Te 3/1/4            Disabled          No
Te 3/2/1            Disabled          No
Te 3/2/2            Disabled          No
Te 3/2/3            Disabled          No
Te 3/2/4            Disabled          No
R3#show gvrp brief
```

Related Commands [show gvrp statistics](#) — displays the GVRP statistics.

show gvrp statistics

Display the GVRP configuration statistics.

Syntax `show gvrp statistics {interface interface | summary}`

Parameters

interface <i>interface</i>	(OPTIONAL) Enter the keyword <code>interface</code> then one of the interface keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.
summary	Enter the keyword <code>summary</code> 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
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
7.6.1.0	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 tengigabitethernet 1/1
```

```
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.



ICMP Message Types

This chapter 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.

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		.

Symbol	Type	Code	Description	Query	Error
&	8	0	echo request	.	
	9	0	router advertisement	.	
	10	0	router solicitation	.	
	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	.	

Internet Group Management Protocol (IGMP)

The IGMP commands are supported by the Dell Networking operating software on the Dell Networking OS.

This chapter contains the following sections:

- [IGMP Commands](#)
- [IGMP Snooping Commands](#)

IGMP Commands

Dell Networking OS supports IGMPv1/v2/v3 and is compliant with RFC-3376.

Important Points to Remember

- Dell Networking OS 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 maximum number of interfaces supported 95.
- 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.

Syntax

```
clear ip igmp [vrf vrf-name] groups [group-address | interface]
```

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 IP multicast group address in dotted decimal format.

interface interface

Enter the following keywords and slot/port[/subport] or number 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.
- 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, refer to the relevant *Dell 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)	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.
8.3.11.1	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.

Syntax `debug ip igmp [vrf vrf-name] [group address | interface]`

- To disable IGMP debugging, use the `no debug ip igmp [vrf vrf-name] [group address | interface]` command.
- To disable all debugging, use the `undebug all` command.

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to enable debugging of IGMP packets corresponding to that VRF.
	 NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.
group-address	(OPTIONAL) Enter the IP multicast group address in dotted decimal format.
interface interface	Enter the following keywords and slot/port[/subport] or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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

Version	Description
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.
8.3.11.1	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 <i>only</i> non-VLAN interfaces — specifying VLAN does not yield results. This command displays packets for IGMP and IGMP snooping.

ip igmp access-group

To specify access control for packets, use this feature.

Syntax	<code>ip igmp access-group access-list</code> To remove the feature, use the <code>no ip igmp access-group access-list</code> command.

Parameters	<i>access-list</i> Enter the name of the extended ACL (16 characters maximum).

Defaults	Not configured
Command Modes	INTERFACE (<i>conf-if-interface-slot/port</i>)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
7.8.1.0	Introduced on the C-Series and S-Series.
7.6.1.0	Introduced on E-Series.

Usage Information The access list accepted is an extended ACL. 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, use this feature.

ip igmp immediate-leave

Enable IGMP immediate leave.

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 <i>prefix-list-name</i>	Enter the keywords <code>group-list</code> then a string up to 16 characters long of the <code>prefix-list-name</code> .

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
9.7(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.
E-Series legacy command	

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.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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)	For IGMP version 2, the Interval range is from 100 to 25599. Introduced on the S6000-ON.
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 query-interval

Change the transmission frequency of IGMP general queries the Querier sends.

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																											
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Maximum range of the Hello interval value is changed to 18000. Introduced on the S6000-ON.</td></tr><tr><td>9.5(0.0)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series in Interface VLAN mode only to enable the system to act as an IGMP Proxy Querier.</td></tr><tr><td colspan="2">E-Series legacy command.</td></tr></table>		Version	Description	9.7(0.0)	Maximum range of the Hello interval value is changed to 18000. Introduced on the S6000-ON.	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.	E-Series legacy command.	
Version	Description																											
9.7(0.0)	Maximum range of the Hello interval value is changed to 18000. Introduced on the S6000-ON.																											
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.																											
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.

 **NOTE:** The IGMP `query-max-resp-time` value must be less than the IGMP `query-interval` value.

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

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(0.0)	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	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.
E-Series legacy command.	

ip igmp ssm-map

To translate (*,G) memberships to (S,G) memberships, use a statically configured list.

Syntax	<code>ip igmp [vrf vrf-name] ssm-map std-access-list source-address</code> Undo this configuration, that is, remove SSM map (S,G) states and replace them with (*,G) state, use the <code>ip igmp [vrf vrf-name] ssm-map std-access-list source-address</code> command.

Parameters	vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> 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.	
	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, refer to the relevant *Dell 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)	Added support for VRF and 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.
7.8.1.0	Introduced on the C-Series and S-Series.
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 version

Manually set the version of the router to IGMPv2 or IGMPv3.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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)	Changed the default IGMP from version 2 to version 3. Introduced on the S6000-ON
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.



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 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.

Syntax `show ip igmp [vrf vrf-name] groups [group-address [detail] | detail | interface [group-address [detail]]]`

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to configure this setting on that VRF.
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[/subport] information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
detail	(OPTIONAL) Enter the keyword <code>detail</code> 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
9.7(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.



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 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 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.

Syntax `show ip igmp [vrf vrf-name] interface [interface]`

Parameters

vrf vrf-name (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to view IGMP interfaces associated with that VRF.

interface (OPTIONAL) Enter the interface type and slot/port[/subport] 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 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, refer to the relevant *Dell 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)	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.
8.3.11.1	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.

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
TenGigabitEthernet 1/1/1 is down, line protocol is down
  Internet protocol processing disabled
TenGigabitEthernet 1/5/1 is down, line protocol is down
  Internet protocol processing disabled
TenGigabitEthernet 1/6/1 is down, line protocol is down
  Internet protocol processing disabled
TenGigabitEthernet 1/7/1 is up, line protocol is down
  Internet protocol processing disabled
Vlan 20
  Inbound IGMP access group is not set
  Internet address is 35.0.0.1/24
  IGMP is enabled on interface
  IGMP query interval is 60 seconds
  IGMP querier timeout is 125 seconds
  IGMP max query response time is 10 seconds
  IGMP last member query response interval is 1000 ms
  IGMP immediate-leave is enabled for all groups
  IGMP activity: 0 joins
  IGMP querying router is 35.0.0.1 (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.

Syntax `show ip igmp [vrf vrf-name] ssm-map [group]`

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> 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	(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, refer to the relevant *Dell 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)	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.
8.3.11.1	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

Dell Networking OS supports IGMP Snooping version 2 and 3 on all Dell Networking systems.

Important Points to Remember for IGMP Snooping

- Dell Networking OS supports version 1, version 2, and version 3 hosts.
- Dell Networking OS 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).
- Dell Networking OS IGMP snooping implementation is based on draft-ietf-magma-snoop-10.
- Dell Networking OS 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.

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 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> 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
9.7(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.

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 <code>snooping</code> 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[/subport] or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> 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
9.7(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.

Syntax

`ip igmp snooping enable`

To disable IGMP snooping, use the `no ip igmp snooping enable` command.

Defaults

Disabled.

Command Modes

- CONFIGURATION
- 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
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9500.



Version	Description
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).



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.

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 VLAN — (conf-if-vl-*n*)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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(0.0)	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.



Version	Description

E-Series legacy
command.

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 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.

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 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
9.7(0.0)	Introduced on the S6000-ON.
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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information This last-member-query-interval is also the interval between successive Group-Specific Query messages. To change the last-member-query interval, use this command.



ip igmp snooping mrouter

Statically configure a VLAN member port as a multicast router interface.

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[/subport] or number 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.

Defaults

Not configured.

Command Modes

INTERFACE VLAN — (conf-if-vl-*n*)

Command History

This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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(0.0)	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command.	

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.

Syntax	<code>ip igmp snooping querier</code> To disable IGMP querier processing for the VLAN interface, use the <code>no ip igmp snooping querier</code> command.
Defaults	Not configured.
Command Modes	INTERFACE VLAN — (conf-if-vl-n)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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(0.0)	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information	This command 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 groups

Display snooping related information for all the IGMP groups, interface or one group of one interface.

Syntax	<code>show ip igmp snooping groups [group-address [detail] detail interface [group-address [detail]]]</code>	
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/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 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, refer to the relevant *Dell 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 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 1/17/1
Dell#
```



show ip igmp snooping mrouter

Display multicast router interfaces.

Syntax `show ip igmp snooping mrouter [vlan number]`

Parameters

vlan number	Enter the keyword <code>vlan</code> 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
9.7(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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command.	

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 1/3/1, Po 1
Dell#
```

Related Commands

- [ip igmp snooping mrouter](#) — configures a static connection to the multicast router.
- [show ip igmp groups](#) — view groups.



Interfaces

The commands in this chapter are supported by Dell Networking operating software on the platform.

This chapter contains the following sections:

- Basic Interface Commands
- Port Channel Commands
- Time Domain Reflectometer (TDR)
- UDP Broadcast

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.

Syntax `clear counters [interface] [vrrp [ipv6 {vrid} | learning-limit | vlan vlan-id]`

Parameters

interface

(OPTIONAL) Enter any of the following keywords and slot/port[/subport] 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 Port Channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For the management interface, enter the keyword `ManagementEthernet` then 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 tunnel interface, enter the keyword `tunnel`. The range is from 1 to 16383.



vrrp [[ipv6] vrid]	(OPTIONAL) Enter the keyword <code>vrrp</code> to clear the counters of all VRRP groups. To clear the counters of VRRP groups on all IPv6 interfaces, enter <code>ipv6</code> . To clear the counters of a specified group, enter a VRID number from 1 to 255.
learning-limit	(OPTIONAL) Enter the keywords <code>learning-limit</code> to clear unknown source address (SA) drop counters when MAC learning limit is configured on the interface.
vlan vlan-id	Enter the keyword <code>vlan</code> followed by 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, refer to the relevant *Dell 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.
9.0.2.0	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.
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 <code>learning-limit</code> option for clarity.

Example

```
Dell#clear counters
Clear counters on all interfaces [confirm]
```

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.

Syntax `clear dampening [interface]`



Parameters

interface (OPTIONAL) Enter any of the following keywords and slot/port[/subport] or number to clear counters from a specified interface:

- 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/subport information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

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, refer to the relevant *Dell 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.
9.0.2.0	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.
8.3.7.0	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 tegigabitethernet 1/10/1
Clear dampening counters on TeGi 1/10/1 [confirm] y
Dell#
```

Related Commands [show interfaces dampening](#) — displays interface dampening information.

[dampening](#) — configures dampening on an interface.

dampening

Configure dampening on an interface.

Syntax

```
dampening [[[half-life] [reuse-threshold]] [suppress-threshold]] [max-suppress-time]]
```



Parameters

<i>half-life</i>	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 .
<i>reuse-threshold</i>	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 .
<i>suppress-threshold</i>	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 .
<i>max-suppress-time</i>	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
9.7(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.
8.3.11.1	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, Dell Networking OS 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-1/10/1)#dampening 20 800 4500 120
Dell(conf-if-te-1/10/1)#
```

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.

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
9.7(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.
8.1.1.0	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.



duplex (10/100 Interfaces)

Configure duplex mode on any physical interfaces where the speed is set to 10/100.

Syntax `duplex {half | full}`

To return to the default setting, use the `no duplex` command.

Parameters

half	Enter the keyword <code>half</code> to set the physical interface to transmit only in one direction.
full	Enter the keyword <code>full</code> to set the physical interface to transmit in both directions.

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
9.7(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.
8.1.1.0	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 This command applies to any physical interface with speed set to 10/100.



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 Mbps or 100 Mbps, you can also execute the `duplex` command.

Related Commands [negotiation auto](#) — enables or disables auto-negotiation on an interface.

flowcontrol

Control how the system responds to and generates 802.3x pause frames.

Syntax `flowcontrol rx {off | on} tx {off | on} [pause- threshold {<1-12480>} [resume-offset <1-12480>}]`

The threshold commands are supported on S6000 only. To return to the default, use the `no flowcontrol rx {off | on} tx {off | on}` threshold command.

Parameters

rx on	Enter the keywords <code>rx on</code> to process the received flow control frames on this port.
rx off	Enter the keywords <code>rx off</code> to ignore the received flow control frames on this port.
tx on	Enter the keywords <code>tx on</code> to send control frames from this port to the connected device when a higher rate of traffic is received.
tx off	Enter the keywords <code>tx off</code> 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 buffer threshold limit for generating PAUSE frames.
resume-offset	Enter the offset value for generating PAUSE frames to resume traffic.

Defaults

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
97(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.
8.1.1.0	Introduced on the E-Series ExaScale.
6.5.1.9 and 7.4.1.0	Introduced on the E-Series.
7.8.1.0	Introduced on the C-Series and S-Series with the <code>thresholds</code> 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.

When a port receives traffic at a higher rate than it can process, the frames are stored in the port buffer. As a result, buffer usage increases. When the buffer usage reaches the value specified in the “pause-threshold” argument, the port sends a PAUSE frame to the connected link partner to stop sending the traffic. Eventually this reduces the buffer usage. When the buffer usage drops by the value specified in the “resume-threshold”, the port again sends a PAUSE frame with 0 as wait-time. This results in resume of the paused traffic flow.

Important Points to Remember

- Do not enable `tx pause` when buffer carving is enabled. For information and assistance, consult Dell Networking TAC.
- 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.**

- Speeds less than 1 Gig cannot be configured when the asymmetric flow control configuration is on. The following error is returned:

Can't configure speed <1G when Asymmetric flowcontrol is on, config ignored

- Dell Networking OS only supports rx on tx on and rx off tx off for speeds less than 1 Gig (Symmetric).

 **NOTE: If you use the disable rx flow control command, Dell Networking recommends rebooting the system.**

Example

```
Dell(conf-if-Te-1/1/1)#show config
!
interface TenGigabitEthernet 1/1/1
no ip address
switchport
no negotiation auto
flowcontrol rx off tx on
no shutdown
...
```

Example (Values)

This Example shows how Dell Networking OS negotiates the flow control values between two Dell Networking chassis connected back-to-back using 1G copper ports.

Configured

LocRxConf	LocTxConf	RemoteRxConf	RemoteTxConf
off	off	off	off
		off	on
		on	off
		on	on
off	on	off	off
		off	on
		on	off
		on	on
on	off	off	off
		off	on
		on	off
		on	on
on	on	off	off
		off	on
		on	off
		on	on

LocNegRx	LocNegTx	RemNegRx	RemNegTx
off	off	off	off
off	off	off	off
off	off	off	off
off	off	off	off
off	off	off	off
off	off	off	off
off	on	on	off
off	off	off	off
off	off	off	off
on	off	off	on
on	on	on	on
on	on	on	on
off	off	off	off

off	off	off	off
on	on	on	on
on	on	on	on

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 interface on the switch.

Syntax

```
interface interface range
```

Parameters

interface

Enter one of the following keywords and slot/port[/subport] or number 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. The slot range is from 1 to 6. The port range is 1.
- 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/subport 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 a number from 1 to 4094.

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, refer to the relevant *Dell 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.
9.4(0.0)	Added the support for interfaces.
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
8.5.1.0	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.

The tunnel interface operates as an ECMP (equal cost multi path) only when the next hop to the tunnel destination is over a physical interface. If you select any other interface as the next hop to the tunnel destination, the tunnel interface does not operate as an ECMP.

Example

```
Dell(config)#int tengigabitethernet 1/10/1
Dell(config-if-te-1/10/1)#exit
Dell(config)#
```

Related Commands

- [interface loopback](#) — configures a Loopback interface.
- [interface null](#) — configures a Null interface.
- [interface port-channel](#) — configures a port channel.
- [interface vlan](#) — configures a VLAN.
- [show interfaces](#) — displays the interface configuration.

interface group

Create or delete group of VLANs with a single command. You can also use this command to apply a set of configurations on a group of interfaces.

Syntax

```
interface group [fortyGigE slot/port { - port } | tengigabitethernet slot/
port/sub-port { - port } | vlan vlanid {- vlanid } ]
```

To delete a range of VLANs, use the following command: `no interface group vlan vlanid {- vlanid}`

Parameters

<i>interface</i> , <i>interface</i> ,...	Enter the keywords <code>interface group</code> and one of the interfaces — slot/port or VLAN number. Select the range of interfaces for bulk configuration. Spaces are not required between the commas. Comma-separated ranges can include VLANs and physical interfaces.



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.

Slot/Port information need not contain a space before and after the dash. For example, both of the following commands are valid: `interface group gigabitethernet 1/1/1 - 5`; `interface group gigabitethernet 1/10/1-5`.

- 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 VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Command Modes CONFIGURATION

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL Switch.

Usage Information The `interface group` command will create all the non-existent VLANs specified in the range. On successful command execution, the CLI switches to the interface group context.

The configuration commands inside the group context will be the similar to that of the existing range command.

Note: For release 9.4(0.0), the group command is supported only for VLANs and physical interfaces.

Example

```
Dell(conf)#interface group ?
fortyGigE          FortyGigabit Ethernet interface
gigabitethernet    GigabitEthernet interface IEEE 802.3z
tengigabitethernet TenGigabit Ethernet interface
vlan               VLAN keyword

Dell(conf)# interface group vlan 1 - 2 , tengigabitethernet 1/10
Dell(conf-if-group-vl-1-2,te-1/1/1)# no shutdown
Dell(conf-if-group-vl-1-2,te-1/1/1)# end
```

Related Commands [interface range](#) — Configures a range of interfaces.
[interface vlan](#) — Configures a VLAN.

interface loopback

Configure a Loopback interface.

Syntax

`interface loopback number`
To remove a loopback interface, use the `no interface loopback number` command.



Parameters	<i>number</i>	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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.4.1.0</td><td>Introduced</td></tr></table>		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.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.4.1.0	Introduced
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.																			
7.6.1.0	Introduced on the S-Series.																			
7.5.1.0	Introduced on the C-Series.																			
6.4.1.0	Introduced																			
Example	<pre>Dell (conf) #interface loopback 1655 Dell (conf-if-lo-1655) #</pre>																			
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).

Syntax	<code>interface ManagementEthernet slot/port[/subport]</code>	
Parameters	<i>slot/port/subport</i>	
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. 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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.11.1	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

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.

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, refer to the relevant *Dell 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.
9.0.2.0	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.
7.6.1.0	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 unreachable`s.

Example

```
Dell(config)#interface null 0
Dell(config-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 unreachable](#)s — 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.

Syntax

```
interface range interface {slot/port[subport] | port} - {slot/port[subport]
| port}, interface {slot/port[subport] | port} - {slot/port[subport] |
port},...
```

Parameters

***interface* {slot/port[subport] | port} — {slot/port[subport] | port}, *interface* {slot/port[subport] | port},...**

Enter `interface range` and one of the interfaces and then slot/port[/subport], port-channel, or VLAN number information. Select the range of interfaces for bulk configuration. You can enter up to six comma-separated ranges. Spaces are not required between the commas. The ranges can include VLANs, port-channels, and physical interfaces.

- 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/subport 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.



Defaults	None
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
8.2.1.0	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[/subport] 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 (...).
- 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)	<pre>Dell(conf)#interface range tengigbitethernet 2/10/1 - 2/11/2, fortyGigbE 3/3, tengigbitethernet 3/10/1 % Warning: Non-existing ports (not configured) are ignored by interface-range</pre>

Example (Multiple Ports)	<pre>Dell(conf)#interface range tengigabitethernet 2/10/1 - 2/20/3, tengigabitethernet 2/11/2 - 2/14/4 Dell(conf-if-range-te-2/10/1-2/20/3)#</pre>

Example (Overlapping Ports)	<pre>Dell(conf)#interface range tengigabitethernet 2/1/1 - 2/10/1, tengigabitethernet 2/1/1 - 2/20/3 Dell(conf-if-range-te-2/1/1-2/20/3)#</pre>



Usage Information	Only VLAN and port-channel interfaces created using the <code>interface vlan</code> and <code>interface port-channel</code> commands can be used in the <code>interface range</code> command. Use the <code>show running-config</code> command to display the VLAN and port-channel interfaces. VLAN or port-channel interfaces that are not displayed in the <code>show running-config</code> command cannot be used with the bulk configuration feature of the <code>interface range</code> command. You cannot create virtual interfaces (VLAN, Port-channel) using the <code>interface range</code> 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 and port-channel only those respective interfaces should be configured in a particular range.
Example (Single Range)	This example shows a single range bulk configuration. <pre>Dell(config)# interface range tengigabitethernet 5/1/1 - 5/7/3 Dell(config-if-range-te-5/1/1-5/7/3)# no shutdown Dell(config-if-range-te-5/1/1-5/7/3)#</pre>
Example (Multiple Range)	This example shows how to use commas to add different interface types to the range enabling all Tengigabit Ethernet interfaces in the range 5/1/1 to 5/20/3 and both Ten-Gigabit Ethernet interfaces 1/1/1 and 1/2/1. <pre>Dell(config-if)# interface range tengigabitethernet 5/1/1 - 5/20/3, tengigabitethernet 1/1/1 - 1/2/1 Dell(config-if-range-te-1/1/1-1/2/1,te-5/1/1-5/20/3)# no shutdown Dell(config-if-range)#</pre>
Example (Multiple Range)	This example shows how to use commas to add VLAN and port-channel interfaces to the range. <pre>Dell(config-if)# interface range tengigabitethernet 5/1/1 -5/20/3, tengigabitethernet 1/1/1 -1/2/1, Vlan 2-100, Port 1-25 Dell(config-if-range-te-1/1/1-1/2/1,te-5/1/1-5/23/1,vl-2-100,po-1-25)# no shutdown Dell(config-if-range)#</pre>
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.

Syntax	<code>define interface range macro <i>name</i> <i>interface</i> , <i>interface</i> , ...</code>
Parameters	<i>name</i> Enter up to 16 characters for the macro name.

interface,
interface,...

Enter the keywords `interface range` and one of the interfaces — slot/port[/subport], 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.

- 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/subport 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 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
9.7(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.
8.5.1.0	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.
pre-Version 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 1/1/1 -3,  
tengigabitethernet 5/1/1 -47, tengigabitethernet 13/1/1 -89
```

```
Dell# show running-config | grep define  
define interface-range test tengigabitethernet 1/1/1 -3,  
tengigabitethernet 5/1/1 -47,  
tengigabitethernet 13/1/1 - 89
```



```
Dell(config)#interface range macro test
Dell(config-if-range-te-1/1/1-3,te-5/1/1-47,te-13/1/1-89) #
```

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.

Syntax `interface range macro name`

Parameters

<i>name</i>	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
9.7(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.
8.1.1.0	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 shows the macro named *test* that was defined earlier.

```
Dell(config)#interface range macro test
Dell(config-if-range-te-1/1/1-1/1/3,te-5/1/1-5/12/1,te-13/1/1-13/22/1) #
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.

Syntax `interface vlan vlan-id [of-instance{of-id}]`

Parameters

<code>of-instance{<i>of-id</i>}</code>	Enter the keyword of-instance then the OpenFlow instance ID to add the VLAN to the specified OpenFlow instance. The range is from 1 to 8.



NOTE: Associate the OpenFlow instance with the VLAN when the VLAN is created. An existing VLAN cannot be associated with an OpenFlow instance.

Defaults Not configured, except for the Default VLAN, which is configured as VLAN 1.

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
9.0.2.0	Introduced on the S6000.
9.1.(0.0)	Introduced on the S4810; added support for OpenFlow.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.

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.

The following features are not supported on VLANs associated with an OpenFlow instance:

- IPv4
- IPv6
- MTU

If OpenFlow VLANs are configured on the switch, spanning-tree protocols cannot be enabled simultaneously.

Example (Single Range)

```
Dell(config)#int vlan 3
Dell(config-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.

intf-type cr4 autoneg

Set the interface type as CR4 with auto-negotiation enabled.

Syntax	<code>intf-type cr4 autoneg</code> If you configure <code>intf-type cr4 autoneg</code> , use the <code>no intf-type cr4 autoneg</code> command to set the interface type as CR4 with autonegotiation disabled.	
Defaults	Not configured	
Command Modes	INTERFACE	
Command History	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.
	8.3.16.1	Introduced on the MXL 10/40GbE Switch IO Module.
Usage Information	If you configure the interface type as CR4 with auto-negotiation enabled, also configure CR4 with auto-negotiation. Many DAC cable link issues are resolved by setting the interface type as CR4. If the CR4 optic fails to come up, use the <code>autoneg</code> option.	
Related Commands	• Interfaces — configures a physical interface. • interface loopback — configures a loopback interface. • interface null — configures a null interface. • interface port-channel — configures a port channel group.	



keepalive

Send keepalive packets periodically to keep an interface alive when it is not transmitting data.

Syntax	<code>keepalive</code> To stop sending keepalive packets, use the <code>no keepalive</code> command.
Defaults	Enabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.

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.
8.1.1.2	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-Version 6.1.1.0	Introduced on the E-Series.

Usage Information	When you configure <code>keepalive</code> , 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 <code>no keepalive</code> , 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.

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.

Syntax	<code>monitor interface [interface]</code> To disable monitoring and return to the CLI prompt, press the <code>q</code> key.		
Parameters	<table><tr><td><i>interface</i></td><td>(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: - For the Management interface on the stack-unit, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 1 to 6. The port range is 1. - For a Tunnel interface, enter the keyword <code>tunnel</code> then the slot/port. The range is from 1 to 16383. </td></tr></table>	<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: - For the Management interface on the stack-unit, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 1 to 6. The port range is 1. - For a Tunnel interface, enter the keyword <code>tunnel</code> then the slot/port. The range is from 1 to 16383.
<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: - For the Management interface on the stack-unit, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 1 to 6. The port range is 1. - For a Tunnel interface, enter the keyword <code>tunnel</code> 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/subport 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.

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
9.0.2.0	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.
8.3.7.0	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.
pre-Version 6.2.1.0	Introduced on the E-Series.

Usage Information

In the Example, the delta column displays changes since the last screen refresh.

The following are the `monitor` command menu options.

Key	Description
systemtest-3	Displays the host name assigned to the system.
monitor time	Displays the amount of time since the <code>monitor interface</code> 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.



Key	Description
T	Increase the screen refresh rate.
t	Decrease the screen refresh rate.
q	Return to the CLI prompt.

Example (Single Interface)

```
systest-3 Monitor time: 00:00:06 Refresh Intvl.: 2s Time: 03:26:26
Interface: te 1/3, Enabled, Link is Up, Linespeed is 1000 Mbit

Traffic statistics:      Current      Rate      Delta
    Input bytes:      9069828    43 Bps      86
    Output bytes:    606915800    43 Bps      86
    Input packets:      54001      0 pps        1
    Output packets:    9401589      0 pps        1
    64B packets:         67      0 pps        0
    Over 64B packets:   49166      0 pps        1
    Over 127B packets:   350      0 pps        0
    Over 255B packets:   1351      0 pps        0
    Over 511B packets:   286      0 pps        0
    Over 1023B packets: 2781      0 pps        0
    Error statistics:
        Input underruns:         0      0 pps        0
        Input giants:           0      0 pps        0
        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
```

```
systest-3 Monitor time: 00:00:06 Refresh Intvl.: 2s Time: 03:26:26
Interface: te 1/3/1, Enabled, Link is Up, Linespeed is 1000 Mbit

Traffic statistics:      Current      Rate      Delta
    Input bytes:      9069828    43 Bps      86
    Output bytes:    606915800    43 Bps      86
    Input packets:      54001      0 pps        1
    Output packets:    9401589      0 pps        1
    64B packets:         67      0 pps        0
    Over 64B packets:   49166      0 pps        1
    Over 127B packets:   350      0 pps        0
    Over 255B packets:   1351      0 pps        0
    Over 511B packets:   286      0 pps        0
    Over 1023B packets: 2781      0 pps        0
    Error statistics:
        Input underruns:         0      0 pps        0
        Input giants:           0      0 pps        0
        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
```



Example (All Interfaces)

systest-3 Monitor time: 00:01:31 Refresh Intvl.: 2s Time: 03:54:14

Interface	Link	In Packets	[delta]	Out Packets	
[delta]					
Te 1/1/1	Down	0	0	0	0
Te 1/1/2	Up	61512	52	66160	42
Te 1/1/3	Up	63086	20	9405888	24
Te 1/1/4	Up	14697471418	2661481	13392989657	
2661385					
Te 1/2/1	Up	3759	3	161959604	832816
Te 1/2/2	Up	4070	3	8680346	5
Te 1/2/3	Up	61934	34	138734357	72
Te 1/2/4	Up	61427	1	59960	1
Te 1/3/1	Up	62039	53	104239232	3
Te 1/3/2	Up	17740044091	372	7373849244	79
Te 1/3/3	Up	18182889225	44	7184747584	138
Te 1/3/4	Up	18182682056	0	3682	1
Te 1/4/1	Up	18182681434	43	6592378911	144
Te 1/4/2	Up	61349	55	86281941	15
Te 1/4/3	Up	59808	58	62060	27
Te 1/4/4	Up	59889	1	61616	1
Te 1/5/1	Up	0	0	14950126	81293
Te 1/5/2	Up	0	0	0	0
Te 1/5/3	Down	0	0	0	0
Te 1/5/4	Up	62734	54	62766	18
Te 1/6/1	Up	60198	9	200899	9
Te 1/6/2	Up	17304741100	3157554	10102508511	
1114221					
Te 1/6/3	Up	17304769659	3139507	7133354895	
523329					
m	- Change mode	c	- Clear screen		
b	- Display bytes	r	- Display pkts/bytes per sec		
l	- Page up	a	- Page down		

mtu

Set the link maximum transmission unit (MTU) (frame size) for an Ethernet interface.

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 9252 for the S6000-ON. The default is **1554**.

Defaults

1554

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
9.7(0.0)	Introduced on the S6000-ON.
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.
7.5.1.0	Introduced on the C-Series.
pre-Version 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, Dell Networking OS 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



negotiation auto

Enable auto-negotiation on an interface.

Syntax `negotiation auto`
To disable auto-negotiation, use the `no negotiation auto` 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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.0	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.
pre-6.2.1.0	Introduced on the E-Series.

Usage Information This command is supported on C-Series, S-Series, and E-Series (TeraScale and ExaScale) 10/100/1000 Base-T Ethernet interfaces.

The `no negotiation auto` command is only available if you first manually set the speed of a port to **10Mbits** or **100Mbits**.

The `negotiation auto` command provides a `mode` option for configuring an individual port to forced-master/forced slave after you enable auto-negotiation.

 **NOTE: The `mode` option is not available on non-10/100/1000 Base-T Ethernet line cards.**

If you do not use the `mode` option, the default setting is **slave**. If you do not configure forced-master or forced-slave on a port, the port negotiates to either a master or a slave state. Port status is one of the following:

- Forced-master
- Force-slave
- Master
- Slave

- Auto-neg Error — typically indicates that both ends of the node are configured with forced-master or forced-slave.



CAUTION: Ensure that one end of your node is configured as forced-master and one is configured as forced-slave. If both are configured the same (that is, forced-master or forced-slave), the `show interfaces` command flaps between an auto-neg-error and forced-master/slave states.

You can display master/slave settings with the `show interfaces` command.

Example (Master/Slave)

```
Dell(conf)# interface tengigabitethernet 1/1/1
Dell(conf-if)#neg auto
Dell(conf-if-autoneg)# ?

end          Exit from configuration mode
exit         Exit from autoneg configuration mode
mode         Specify autoneg mode
no           Negate a command or set its defaults
show         Show autoneg configuration information
Dell(conf-if-autoneg)#mode ?
forced-master Force port to master mode
forced-slave  Force port to slave mode
Dell(conf-if-autoneg)#
```

Example (Configured)

```
Dell#show interfaces configured
TenGigabitEthernet 13/3/4 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:fc
  Current address is 00:01:e8:05:f7:fc
  Interface index is 474791997
  Internet address is 1.1.1.1/24
  MTU 1554 bytes, IP MTU 1500 bytes
  LineSpeed 1000 Mbit, Mode full duplex, Master
  ARP type: ARPA, ARP Timeout 04:00:00
  Last clearing of "show interfaces" counters 00:12:42
  Queueing strategy: fifo
  Input Statistics:
  ...
```

User Information

Both sides of the link must have auto-negotiation enabled or disabled for the link to come up.

The following details the possible speed and auto-negotiation combinations for a line between two 10/100/1000 Base-T Ethernet interfaces.

Port 0

- auto-negotiation enabled* speed 1000 or auto
- auto-negotiation enabled speed 100
- auto-negotiation disabled speed 100
- auto-negotiation disabled speed 100
- auto-negotiation enabled* speed 1000 or auto

Port 1

- auto-negotiation enabled* speed 1000 or auto
- auto-negotiation enabled speed 100
- auto-negotiation disabled speed 100
- auto-negotiation enabled speed 100
- auto-negotiation disabled speed 100

Link Status Between Port 1 and Port 2



- Up at 1000 Mb/s
- Up at 100 Mb/s
- Up at 100 Mb/s
- Down
- Down

* You cannot disable auto-negotiation when the speed is set to 1000 or auto.

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.

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 (conf-if-interface-slot/port[/subport])

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.
7.6.1.0	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 tengigabitethernet 7/1/1
Dell(conf-if-gi-7/0)#portmode hybrid
Dell(conf-if-gi-7/0)#interface vlan 10
Dell(conf-if-vl-10)#untagged tengigabitethernet 7/1/1
Dell(conf-if-vl-10)#interface vlan 20
Dell(conf-if-vl-20)#tagged tengigabitethernet 7/1/1
Dell(conf-if-vl-20)#
```

Example

```
Dell(conf-if-vl-20)#do show interfaces switchport
Name: TenGigabitEthernet 7/1/1
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 tengigabitethernet 7/1/1
Dell(conf-if-vl-10)#interface vlan 20
Dell(conf-if-vl-20)#no tagged tengigabitethernet 7/1/1
Dell(conf-if-vl-20)#interface tengigabitethernet 7/1/1
Dell(conf-if-gi-7/0)#no portmode hybrid
Dell(conf-if-vl-20)#
```

rate-interval

Configure the traffic sampling interval on the selected interface.

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
9.7(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.
8.1.1.0	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.

show config

Display the interface configuration.

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
9.0.2.0	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-Version 6.2.1.0	Introduced on the E-Series.

Example

```
Dell(conf-if-fo-1/4)#show config
!
interface fortyGigE 1/4
no ip address
mtu 12000
switchport
```

```
no shutdown
Dell(conf-if-fo-1/4) #
```

show config (for speed)

Syntax `show config`

Command Modes INTERFACE MODE

Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.3(0.1)	Introduced on the S6000.

Usage Information In order for the speed information corresponding to an interface to appear in the show command output, you must first configure the speed of that interface using the `speed` command.

Example

```
Dell(conf-if-te-1/1/1)#speed ?
100                100 Mbps
1000               1000 Mbps
10000              10000 Mbps
auto               Auto negotiation (default)
Dell(conf-if-te-1/1/1)#speed 100
Dell(conf-if-te-1/1/1)#show config
interface TenGigabitEthernet 1/1/1
speed 100
no shutdown
```

show config (from INTERFACE RANGE mode)

Display the bulk configured interfaces (`interface range`).

Syntax `show config`

Command Modes CONFIGURATION INTERFACE (conf-if-range)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.
7.6.1.0	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.

Example

```
Dell(conf)#interface range tengigabitethernet 1/1/1 - 1/1/2
Dell(conf-if-range-gi-1/1-1/1/2)#show config
!
interface TenGigabitEthernet 1/1/1
  no ip address
  switchport
  no shutdown
!
interface TenGigabitEthernet 1/1/2
  no ip address
  switchport
  no shutdown
Dell(conf-if-range-gi-1/1-1/1/2)#
```

show interfaces

Display information on a specific physical interface or virtual interface.

Syntax `show interfaces interface`

Parameters

interface

Enter one of the following keywords and slot/port[/subport] or number information:

- For a Loopback interface, enter the keyword `loopback` then a number from 0 to 16383.
- For stack-units, enter the keywords `stack-unit` then the slot/port information.
- For a Null interface, enter the keyword `null` then the Null interface number.
- 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/subport 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.

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
9.2(0.2)	Added support for the tunnel interface type.



Version	Description
9.1(0.0)	Updated Management Ethernet 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.

-  **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.

User Information The following table describes the `show interfaces` command shown in the 10G (TeraScale) Example.

Line	Description
TenGigabitEthernet 1/1...	Interface type, slot/port/subport, 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 Dell Networking allows unsupported SFP and XFP transceivers to be used, but Dell Networking OS 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

Line	Description
	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 the SNMP uses 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 negotiation mode.
ARP type:...	Displays the ARP type and the ARP timeout value for the interface.
Last clearing...	Displays the time when the <code>show interfaces</code> counters were 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 runs, giants, and throttles packets: – runs = 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 runs, 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 the 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: – Vlan = 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 2/1 is down, line protocol is down
Hardware is DellForce10Eth, address is 00:01:e8:8b:3d:e7
Current address is 00:01:e8:8b:3d:e7
Pluggable media present, Media type is unknown
Wavelength unknown
Interface index is 100992002
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto
Flowcontrol rx on tx off
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 3d17h53m
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 runs, 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 wredrops
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: 3d17h51m
```

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.

Example (1G SFP)

```
Dell#show interfaces tengigabitethernet 2/1/1
TenGigabitEthernet 2/1/1 is up, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:41:77:95
Current address is 00:01:e8:41:77:95
Pluggable media present, SFP type is 1000BASE-SX
Wavelength is 850nm
Interface index is 100974648
Port will not be disabled on partial SFM failure
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit
Flowcontrol rx on tx on
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 1w0d5h
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  0 Vlans
```



```

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 runs, 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 Vlans, 0 throttles, 0 discarded, 0 collisions, 0 wredrops
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: 1w0d5h
Dell#

```

**Example
(Management
Ethernet)**

```

Dell#show interfaces managementethernet 1/1/1

ManagementEthernet 1/1/1 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:0b:a9:4c
Current address is 00:01:e8:0b:a9:4c
Pluggable media not present
Interface index is 503595208
Internet address is 10.11.201.5/16
Link local IPv6 address: fe80::201:e8ff:fe0b:a94c/64
Global IPv6 address: 2222::5/64
Virtual-IP is not set
Virtual-IP IPv6 address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 10 Mbit, Mode half duplex
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 04:01:08
Queueing strategy: fifo
Input 943 packets, 78347 bytes, 190 multicast
Received 0 errors, 0 discarded
Output 459 packets, 102388 bytes, 15 multicast
Output 0 errors, 0 invalid protocol
Time since last interface status change: 00:03:09

```

**Example
(Management
Ethernet, two IPv6
addresses)**

```

Dell#show interfaces managementethernet 1/1/1

ManagementEthernet 1/1/1 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 (OpenFlow instance)

```

Dell#show interfaces vlan 6

Vlan 6 is down, line protocol is down

Address is 00:01:e8:8a:e1:8c, Current address is 00:01:e8:8a:e1:8c

Interface index is 1107525638

of-instance: 2

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 00:05:12

Queueing strategy: fifo

Time since last interface status change: 00:05:12

```

Related Commands

[show interfaces configured](#) – displays any interface with a non-default configuration.

[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 range](#) – displays all interfaces configured using the interface range command.



show interfaces configured

Display any interface with a non-default configuration.

Syntax `show interfaces configured`

Command Modes

- EXEC
- EXEC Privilege

Command History	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.
	8.1.1.0	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.

Example

```
Dell#show interfaces configured
TenGigabitEthernet 9/18/1 is up, line protocol is up
Hardware is Force10Eth, address is 00:01:e8:05:f7:fc
  Current address is 00:01:e8:05:f7:fc
Interface index is 474791997
Internet address is 1.1.1.1/24
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed 1000 Mbit, Mode full duplex, Master
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interfaces" counters 00:12:42
Queueing strategy: fifo
Input Statistics:
  10 packets, 10000 bytes
  0 Vlans
  0 64-byte pkts, 0 over 64-byte pkts, 0 over 127-byte pkts
  0 over 255-byte pkts, 10 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:
  1 packets, 64 bytes, 0 underruns
  1 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, 1 Broadcasts, 0 Unicasts
  0 Vlans, 0 throttles, 0 discarded, 0 collisions
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: 00:04:59
Dell#
```

Related Commands [show interfaces](#) — displays information on a specific physical interface or virtual interface.



show interfaces dampening

Display interface dampening information.

Syntax `show interfaces dampening [[interface] [summary] [detail]]`

Parameters

<i>interface</i>	(Optional) Enter one of the following keywords and slot/port[/subport] or number information: - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
<i>summary</i>	(OPTIONAL) Enter the keyword <code>summary</code> to display the current summary of dampening data, including the number of interfaces configured and the number of interfaces suppressed, if any.
<i>detail</i>	(OPTIONAL) Enter the keyword <code>detail</code> to display detailed interface dampening data.

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
9.7(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.
8.5.1.0	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

Example

```
Dell#show interfaces dampening
Interface Supp   Flaps Penalty Half-Life Reuse Suppress Max-Sup
          State
Te 3/2/1      Up      0      0         20       800    4500     120
```



```

Te 3/10/1   Up      0      0      5      750    2500    20
Dell#

```

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 stack-unit

Display information on all interfaces on a specific S-Series or Z-Series stack member.

Syntax `show interfaces stack-unit unit-number`

Parameters

<i>unit-number</i>	Enter the stack member number.

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
9.7(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.

Example

```

Dell#show interfaces stack-unit 1
TenGigabitEthernet 1/1/1 is down, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:4c:f2:82
Current address is 00:01:e8:4c:f2:82
Pluggable media not present
Interface index is 34129154
Internet address is not set
MTU 1554 bytes, IP MTU 1500 bytes
LineSpeed auto, Mode auto
ARP type: ARPA, ARP Timeout 04:00:00
Last clearing of "show interface" counters 3w0d17h
Queueing strategy: fifo
Input Statistics:
  0 packets, 0 bytes
  5144 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 runs, 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
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: 3w0d17h
GigabitEthernet 1/1/2 is down, line protocol is down
Hardware is Force10Eth, address is 00:01:e8:4c:f2:83
  Current address is 00:01:e8:4c:f2:83
!-----output truncated -----!

```

Related Commands [show hardware stack-unit](#) — displays data plane and management plane input/output statistics.

[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 stack-unit slot and interface.

Syntax `show interfaces [interface status`

Parameters

interface (OPTIONAL) Enter one of the following keywords and slot/port[/subport] or number 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 the slot/port information. The range is from 0 to 16383.
- For a port channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.5.1.0	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.

Example

```
Dell#show interfaces status
Port      Description  Status  Speed    Duplex  Vlan
Te 1/1/1                                Up      1000 Mbit Auto   --
Te 1/2/1                                Down    Auto    Auto    1
Te 1/3/1                                Down    Auto    Auto    1
Te 1/4/1                                Down    Auto    Auto    --
Te 1/5/1  DellPort  Up      1000 Mbit Auto    30-130
Te 1/6/1                                Down    Auto    Auto    --
Te 1/7/1                                Down    Auto    Auto    --
Te 1/8/1                                Up      1000 Mbit Auto    1502,1504,1506-1508,1602
Te 1/9/1                                Down    Auto    Auto    --
Te 1/10/1                               Down    Auto    Auto    --
Te 1/11/1                               Down    Auto    Auto    --
Te 1/12/1                               Down    Auto    Auto    --
Te 1/13/1                               Down    Auto    Auto    --
Te 1/14/1                               Down    Auto    Auto    --
Te 1/15/1                               Down    Auto    Auto    --
Te 1/16/1                               Down    Auto    Auto    -Dell#
```

Related Commands [show interfaces](#) — displays information on a specific physical interface or virtual interface.

show interfaces vlan

Display VLAN statistics.

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
9.7(0.0)	Introduced on the S-Series and Z-Series.

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 system stack-unit quad-port-profile

Displays the list of configured and activated dynamic fan-out capable ports.

Syntax `show system [stack-unit-number] quad-port-profile`

Parameters *stack-unit number* Enter the port number. The range is from 1–6.

Command Modes EXEC Privilege

Command History	Version	Description
	9.7(0.0)	Introduced on the S6000 and S6000-ON.

Example

```

Dell#show system stack-unit 1 quad-port-profile
Configured fan out profile ports in stack-unit 1
    Configured      Activated
         2             2
         4             4
         6             6
         8             8
         9             9
        10            10
        11            11
        12            12
        13            13
        14            14
        15            15
        16            16
        17            17
        18            18
        19            19
        20            20
        21            21
        22            22
        23            23
        24            24
        25            25
        27            27
        29            29
        31            31

```

```

Dell(conf)#stack-unit 1 port 24 portmode quad
Warning: Enabling quad mode on stack-unit 1 port 24. Please verify whether
the configs related to interface Fo 1/24 are cleaned up before proceeding
further.
[confirm yes/no]:yes

```



```

Dell(conf)#00:02:24: %STKUNIT1-M:CP %IFMGR-5-DYNAMIC_FANOUT: Port 24 in
slot 1 has been fanned-out >>>>
Dell(conf)#00:02:27: %S6000-ON:1 %IFAGT-5-INSERT_OPTICS_QSFP: Optics QSFP
inserted in slot 1 port 24/2
00:02:27: %S6000-ON:1 %IFAGT-5-INSERT_OPTICS_QSFP: Optics QSFP inserted in
slot 1 port 24/3
i00:02:27: %S6000-ON:1 %IFAGT-5-INSERT_OPTICS_QSFP: Optics QSFP inserted
in slot 1 port 24/4

```

Related Commands [stack-unit portmode](#) — splits a single 40G port into four-10G ports

stack-unit quad-port-profile

Configures the list of dynamic fan-out capable ports.

Syntax	<code>stack-unit [stack-unit number] quad-port-profile [default <1-32>]</code> To remove the quad-port configuration, use the <code>[no] stack-unit[stack-unit number] quad-port-profile [default <1-32>]</code> command syntax.	
Parameters	stack-unit number<1-32>	Enter the port number. The range is from 1 to 6. The range of the default ports are separated by —,
Defaults	2,4,6,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,27,29,31	
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000 and S6000-ON.
Usage Information	The profile can only have 12-port groups in the first 16 and last 16 groups. Any change in the profile needs <i>save</i> and <i>reload</i> .	

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.

Syntax	<code>show interfaces switchport [interface stack-unit unit-id]</code>	
Parameters	<i>interface</i> (OPTIONAL) Enter one of the following keywords and slot/port[/subport] or number information: - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a backup interface for this interface, enter the keyword <code>backup</code>.	



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
9.7(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.
8.5.1.0	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.
E-Series legacy command	

Usage Information

The following describes the `show interfaces switchport` command for the following example.

Items	Description
Name	Displays the interface's type, slot/port[/subport] 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. Starting with Dell Networking OS version 7.6.1, this field can display native VLAN membership by port 13/0.

Example

```
Dell#show interfaces switchport
Name: TenGigabitEthernet 13/1/1
802.1QTagged: Hybrid
Vlan membership:
Vlan    2, Vlan 20
Native VlanId: 20

Name: TenGigabitEthernet 13/2/1
802.1QTagged: True
Vlan membership:
Vlan    2

Name: TenGigabitEthernet 13/3/1
802.1QTagged: True
Vlan membership:
Vlan    2

Name: TenGigabitEthernet 13/4/1
802.1QTagged: True
```



```
Vlan membership:
Vlan    2
--More--
```

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.

Syntax `show interfaces [tengigabitethernet slot/port[/subport] | fortyGigE slot/port] transceiver`

Parameters

tengigabitethernet	For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information.
fortyGigE	For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> 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
9.7(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.
8.5.1.0	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.
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 used by SNMP 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+.
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+.



Line	Description
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.

Example

```

Dell#show interfaces TengigabitEthernet 1/1/1 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 Transceiver 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 -----

```

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 inventory \(S-Series and Z-Series\)](#) — displays the switch type, components (including media), Dell Networking OS version including hardware identification numbers and configured protocols.

show range

Display all interfaces configured using the `interface range` command.

Syntax	<code>show range</code>
Command Modes	INTERFACE RANGE (config-if-range)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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	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-if-range-te-2/2/1,fo-2/56)#show range
2/2/1 - 0
2/56 - 0
Dell(conf-if-range-te-2/2/1,fo-2/56)#
```

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.

shutdown

Disable an interface.

Syntax	<code>shutdown</code> To activate an interface, use the <code>no shutdown</code> 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
9.7(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.
8.1.1.0	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 legacy
command**

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 (Management interface)

Set the speed for the Management interface.

Syntax `speed {10 | 100 | 1000 | auto}`

To return to the default setting, use the `no speed` 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.



1000	Enter the keyword <code>1000</code> to set the interface to auto-negotiate its speed.
auto	Enter the keyword <code>auto</code> 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
9.7(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.
8.3.11.1	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.
pre-Version 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).

[duplex \(10/100 Interfaces\)](#) — configures duplex mode on physical interfaces with the speed set to 10/100.

[management route](#) — configures a static route that points to the Management interface or a forwarding router.

stack-unit portmode

You can split a single 40G port into four-10G portsYou can split a single 40G port into four 10G ports without reload..

Syntax `stack-unit stack-unit port number portmode quad`

Parameters

stack-unit	Enter the stack member unit identifier of the stack member to reset. For the S6000-ON, the range is from 1 to 5.
number	Enter the port number of the 40G port to be split. The total number of ports are 32. The range is from 1 to 32.

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
9.7(0.0)	Added support for dynamically fanning-out of interfaces on S6000. 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.
8.3.7.1	Introduced on the S4810.

Usage Information

Splitting a 40G port into 4x10G port is supported on standalone and stacked units. `stack-unit stack-unit port number portmode quad` dynamically fan-out 40G ports to 10G ports and vice-versa without reload in S6000 and S6000-ON switch.

The quad port must be in a default configuration before it can be split into 4x10G ports. The 40G port is lost in the config when the port is split, so be sure that the port is also removed from other L2/L3 feature configurations.

This command cannot be used if LR4 optics are inserted on the 40G interface.

The following guidelines apply to the splitting of 40GbE QSFP+ ports into four 10GbE SFP+ ports by using the `stack-unit portmode` command on the S6000 or S6000-ON platform.

- For S6000-ON, the default ports on quad-port-profile are 2,4,6,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,27,29,31. For example, `stack-unit 1 quad-port-profile 2,4,6,8,9,10,11,12,13,14,15,16,17,18,19,20,21,22,23,24,25,27,29,31`.

Example (stack unit – Warning message when 13 ports are configured in any port range)

```
Dell(conf)#stack-unit 0 port 48 portmode quad
Maximum number of ports that can be made Quad mode in the range <0-63> is
configured. Ports 52,56,60, will be disabled on reload.
Do you wish to continue? [confirm yes/no]:yes
Please save and reset unit 0 for the changes to take effect.
Dell(conf)#
```

switchport

Place an interface in Layer 2 mode.

Syntax

```
switchport [backup interface {gigabit slot/port[/subport] | tengigabit
slot/port[/subport] | 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 {gigabit slot/port[/subport] | tengigabit slot/port[/subport] | 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 <code>backup interface</code> 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 <code>tengigabit</code> if the backup port is a 10G port.
fortyGigE	Enter the keyword <code>fortyGigE</code> if the backup port is a 40G port.
port-channel	Enter the keywords <code>port-channel</code> if the backup port is a static or dynamic port channel.
slot/port[/subport]	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, refer to the relevant *Dell 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.
9.0.2.0	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 for port-channel interfaces (the <code>port-channel number</code> 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 <code>backup interface</code> option.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-Version 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, refer to the “Configuring Redundant Links” section in the “Layer 2” chapter of the *Dell Networking OS Configuration Guide*.



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 referred to as a Port Channel.

- For the S-Series and Z9000, the maximum port channel ID is 128 and the maximum members per port channel is 16.

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. In the S-Series, stack members can provide those ports.

 **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, refer to the [Link Aggregation Control Protocol \(LACP\)](#) chapter. For more information about configuring and using Port Channels, refer to the *Dell Networking OS Configuration Guide*.

channel-member

Add an interface to the Port Channel, while in INTERFACE PORTCHANNEL mode.

Syntax	<code>channel-member interface</code> To delete an interface from a Port Channel, use the <code>no channel-member interface</code> command.	
Parameters	<i>interface</i>	(OPTIONAL) Enter any of the following keywords and slot/port[/subport] or number information: • For a 100/1000 Ethernet interface, enter the keyword <code>GigabitEthernet</code> then the slot/port[/subport] information. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
Defaults	Not configured.	
Command Modes	INTERFACE PORTCHANNEL	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.
8.3.7.0	Introduced on the S4810.
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.
pre-Version 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.

You can have 16 interfaces per Port Channel on the S-Series and Z-Series. The interfaces can be located on different line cards but must be the same physical type and speed (for example, all 1-Gigabit Ethernet interfaces). However, you can combine 100/1000 interfaces and GE interfaces in the same Port Channel.

If the Port Channel contains a mix of interfaces with 100 Mb/s speed and 1000 Mb/s speed, the software disables those interfaces whose speed does not match the speed of the first interface configured and enabled in the Port Channel. If that first interface goes down, the Port Channel does not change its designated speed; disable and re-enable the Port Channel or change the order of the channel members configuration to change the designated speed. If the Port Channel contains a mix of interfaces with 100 Mb/s speed and 1000 Mb/s speed, the software disables those interfaces whose speed does not match the speed of the first interface configured and enabled in the Port Channel. If that first interface goes down, the Port Channel does not change its designated speed; disable and re-enable the Port Channel or change the order of the channel members configuration to change the designated speed. For more information about Port Channels, refer to the *Dell Networking OS Configuration Guide*.

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").

Syntax `group group_number port-channel number port-channel number`



To remove an existing LAG supergroup, use the `no group group_number` command.

Parameters	<i>group_number</i>	Enter an integer from 1 to 32 that uniquely identifies this LAG fate-sharing group.
	<i>port-channel number</i>	Enter the keywords <code>port-channel</code> 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
9.7(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.
8.1.1.0	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 16 physical interfaces on the S-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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
Version 9.0.2.0	Introduced on the S6000.
Version 8.3.19.0	Introduced on the S4820T.
Version 8.3.12.0	Introduced on S4810.
Version 8.3.11.1	Introduced on Z9000.
Version 8.1.1.0	Introduced on E-Series ExaScale.
Version 7.6.1.0	Introduced on S-Series.
Version 7.5.1.0	Introduced on C-Series.
pre-Version 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). You can add a Port Channel in Layer 2 mode to a VLAN.

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, Dell Networking OS 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 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.

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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-Version 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.

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
9.7(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.
8.1.1.0	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 interfaces port-channel

Display information on configured Port Channel groups.

Syntax `show interfaces port-channel [channel-number] [brief]`

Parameters

channel-number	For a Port Channel interface, enter the keyword <code>port-channel</code> then a number. For the C-Series and S-Series, the range is from 1 to 128.
brief	(OPTIONAL) Enter the keyword <code>brief</code> 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, refer to the relevant *Dell 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.



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.
7.6.1.0	Introduced on the S-Series. Modified to display the LAG failover group status.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Usage Information 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 <code>show interfaces</code> 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.



Field	Description
Time since...	Displays the time since the last change in the configuration of this interface.

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: Gi 2/5 Gi 2/18
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#

```

User 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). • 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#show interfaces port-channel 1 brief

LAG Mode Status Uptime    Ports

```



```

1    L2    up      00:00:08  Te 3/1/1  (Up) *
                                Te 3/2/1  (Down)
                                Te 3/3/1  (Up)
Dell#

```

Related Commands [show lacp](#) — displays the LACP matrix.

show port-channel-flow

Display an egress port in a given port-channel flow.

Syntax

```

show port-channel-flow outgoing-port-channel number incoming-interface
interface {source-ip address destination-ip address} | {source-port number
destination-port number} | {source-mac address destination-mac address
{vlan vlanid | ether-type}}

```

Parameters

outgoing-port-channel <i>number</i>	Enter the keywords <code>outgoing-port-channel</code> then the number of the port channel to display flow information. For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.
incoming-interface <i>interface</i>	Enter the keywords <code>incoming-interface</code> then the interface type and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
source-ip <i>address</i>	Enter the keywords <code>source-ip</code> then the IP source address in IP address format.
destination-ip <i>address</i>	Enter the keywords <code>destination-ip</code> then the IP destination address in IP address format.
source-port <i>number</i>	Enter the keywords <code>source-port</code> then the source port number. The range is from 1 to 65536. The default is None .
destination-port <i>number</i>	Enter the keywords <code>destination-port</code> then the destination port number. The range is from 1 to 65536. The default is None .
source-mac <i>address</i>	Enter the keywords <code>source-mac</code> then the MAC source address in the nn:nn:nn:nn:nn:nn format.
destination-mac <i>address</i>	Enter the keywords <code>destination-mac</code> then the MAC destination address in the nn:nn:nn:nn:nn:nn format.
vlan <i>vlan-id</i>	Enter the keywords <code>vlan</code> then the VLAN-id. The range is from 0 to 4094.
ether-type	Enter the keywords <code>ether-type</code> in the XX:XX format.

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
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	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

Enhanced Validation of Interface Ranges

This functionality is supported on the platform.

You can avoid specifying spaces between the range of interfaces, separated by commas, that you configure by using the `interface range` command. For example, if you enter a list of interface ranges, such as `interface range fo 1/1-1,te 2/1/1`, this configuration is considered valid. The comma-separated list is not required to be separated by spaces in between the ranges. You can associate multicast MAC or hardware addresses to an interface range and VLANs by using the `mac-address-table static multicast-mac-address vlan vlan-id output-range interface` command.

ip http source-interface

Specify an interface as the source interface for HTTP connections.

This feature is supported on platform.



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 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 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

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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

Related Commands

ip ftp source interface

Configuring source interface for ftp communications.



IPv4 Routing

The basic IPv4 commands are supported by Dell Networking operating system on the platform.

arp

To associate an IP address with a MAC address in the switch, use address resolution protocol (ARP).

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 <code>arp</code> 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	(OPTIONAL) Enter any of the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For the Management interface on the stack-unit, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 1 to 6. The port range is 1. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.

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.
9.4(0.0)	Added support for VRF.



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.
8.5.1.0	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.
pre-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.

You can use the `vrf` attribute of this command to create a static ARP entry on either a default or a non-default VRF. You cannot use this parameter to create any static ARPs corresponding to management VRFs. When a VRF is deleted using the `no ip vrf` command, all the static ARP configurations that belong to that VRF are removed automatically.

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.

Syntax `arp backoff-time seconds`

Parameters

seconds	Enter the number of seconds an ARP entry is black-holed. The range is from 1 to 3600. The default is 30 .

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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.3.8.0	Introduced on the S4810.

Usage Information This 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.

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
9.7(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.
8.3.1.0	Introduced.

Usage Information In Dell Networking OS versions prior to 8.3.1.0, if a gratuitous ARP is received some time after an ARP request is sent, only RP2 installs the ARP information. For example:

1. At time $t=0$, Dell Networking OS sends an ARP request for IP *A.B.C.D*.
2. At time $t=1$, Dell Networking OS receives an ARP request for IP *A.B.C.D*.
3. At time $t=2$, Dell Networking OS installs an ARP entry for *A.B.C.D* only on RP2.

Beginning with Dell Networking OS version 8.3.1.0, when a gratuitous ARP is received, Dell Networking OS installs an ARP entry on all three CPUs.



arp max-entries

Enables you to configure the maximum number of ARP entries per VRF that are allowed for IPv4..

Syntax	<code>arp max-entries [vrf vrf-name] max-number</code>	
Parameters	<i>vrf vrf-name</i>	Enter the name of a specific VRF for which you want to configure maximum number of ARP entries that IPv4 allows.
	<i>max-number</i>	Enter the maximum number of ARP entries that a VRF RTM can hold. The range is from 0 to 65535.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	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.
	9.4.(0.0)	Introduced on the S4810 and S4820T.
Usage Information	Use this command to specify the maximum number of ARP entries that the Route Table Manager can hold for a specific VRF. This command does not apply to the management VRFs.	

arp retries

Set the number of ARP retries in case the system does not receive an ARP reply in response to an ARP request.

Syntax	<code>arp retries number</code>	
Parameters	<i>number</i>	Enter the number of retries. The range is from 1 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 <i>Dell Networking OS Command Line Reference Guide</i> .	
	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.



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.
8.3.1.0	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.

Syntax `arp timeout minutes`

Parameters

<i>minutes</i>	Enter the number of minutes. The range is from 0 to 35790. The default is 240 minutes .

Defaults **240 minutes** (4 hours)

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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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).

Syntax `clear arp-cache [vrf vrf-name | interface | ip ip-address] [no-refresh]`

Parameters

- vrf vrf-name** (OPTIONAL) Enter the keyword `vrf` and then the name of the VRF to clear the ARP cache corresponding to that VRF.
- interface** (OPTIONAL) Enter the following keywords and slot/port[/subport] or number 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 the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 1 to 6. The port range is 1.
 - 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.
- 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 re-installed 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
9.7(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.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.

Version	Description
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-6.2.1.1	Introduced on the E-Series.

clear host

Remove one or all dynamically learned host table entries.

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
9.7(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.
8.1.1.0	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 stack-unit

Clear all FIB entries in the specified stack unit (use this command with caution, refer to *Usage Information*.)

Syntax `clear ip fib stack-unit unit-number vrf vrf-name`



Parameters	<i>unit-number</i>	Enter the number of the stack unit.
	<i>vrf vrf-name</i>	Enter the keyword <code>vrf</code> followed by the name of the VRF to clear all FIB entries corresponding to that VRF.
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	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.
	9.4(0.0)	Added support for VRF.
	9.0.2.0	Introduced on the S6000.
	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	<code>show ip fib stack-unit</code> — shows FIB entries on a specified stack-unit.	

clear ip route

Clear one or all routes in the routing table.

Syntax	<code>clear ip route [vrf vrf-name] { * ip-address mask }</code>	
Parameters	*	Enter an asterisk (*) to clear all learned IP routes.
	<i>ip-address mask</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	
	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.

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.
7.9.1.0	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-6.2.1.1	Introduced on the E-Series.

Usage Information Use the `vrf vrf-name` attribute of this command to clear routes corresponding to either a specific VRF or the default VRF.

You cannot use this attribute to clear routes corresponding to a management VRF.

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 tcp statistics

Clear TCP counters.

Syntax `clear tcp statistics [all | cp | rp1 | rp2]`

Parameters

all	Enter the keyword <code>all</code> to clear all TCP statistics maintained on all switch processors.
cp	(OPTIONAL) Enter the <code>cp</code> to clear only statistics from the Control Processor.
rp1	(OPTIONAL) Enter the keyword <code>rp1</code> to clear only the statistics from Route Processor 1.
rp2	(OPTIONAL) Enter the keyword <code>rp2</code> to clear only the statistics from Route Processor 2.

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
9.7(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.
pre-6.2.1.1	Introduced on the E-Series.

debug arp

View information on ARP transactions.

Syntax

```
debug arp [interface] [count value]
```

To stop debugging ARP transactions, use the `no debug arp` command.

Parameters

<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For the Management interface on the stack-unit, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 1 to 6. The port range is 1. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
<i>count value</i>	(OPTIONAL) Enter the keyword <code>count</code> 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
9.7(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.
8.5.1.0	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 <code>count</code> 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.

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
9.7(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.
8.5.1.0	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.



Version	Description
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.4.1.0	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,
giaddr = 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,
giaddr = 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,
giaddr = 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, giaddr =
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,
giaddr = 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, giaddr =
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).

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[/subport] or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For the Management interface on the stack-unit, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 1 to 6. The port range is 1. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
count value	(OPTIONAL) Enter the keyword <code>count</code> 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
9.7(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.
8.5.1.0	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 <code>count</code> 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.

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[/subport] or number 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 the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 1 to 6. The port range is 1.
 - 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.

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
9.7(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.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.



Version	Description
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 <code>access-group</code> 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 <code>count</code> 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 1/1), len 54, sending
    TCP src=23, dst=40869, seq=2112994894, ack=606901739, win=8191 ACK PUSH
IP: s=10.1.2.206 (Ma 1/1), 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 1/1), len 226, sending
    TCP src=23, dst=40869, seq=2112994896, ack=606901739, win=8192 ACK PUSH
IP: s=10.1.2.216 (Ma 1/1), 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 1/1), 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 1/1), len 1500, sending fragment
    IP Fragment, Ident = 4741, fragment offset = 1480
IP: s=40.40.40.40 (local), d=224.0.0.5 (Te 4/11/1), len 64, sending broad/
multicast
proto=89
IP: s=40.40.40.40 (local), d=224.0.0.6 (Te 4/11/1), 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`)

In the case of ambiguous access control list rules, the `debug ip packet access-control` command is disabled. A message appears identifying the error (refer to the Example below).

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#
```

ip address

Assign a primary and secondary IP address to the interface.

Syntax

```
ip address ip-address mask [secondary]
```

To delete an IP address from an interface, use the `no ip address [ip-address]` command.

Parameters

<i>ip-address</i>	Enter an IP address in dotted decimal format.
<i>mask</i>	Enter the mask of the IP address in slash prefix format (for example, /24).
<i>secondary</i>	(OPTIONAL) Enter the keyword <code>secondary</code> to designate the IP address as the secondary address.

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
9.7(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.
8.1.1.0	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

Enables the interface to receive directed broadcast packets.

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
9.7(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.
8.1.1.0	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.

ip domain-list

Configure names to complete unqualified host names.

Syntax `ip domain-list name`
 To remove the name, use the `no ip domain-list name` command.

Parameters **name** Enter a domain name to be used 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
9.7(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.
8.1.1.0	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

To address resolution (that is, DNS), enable dynamic host-name.

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
9.7(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.
8.1.1.0	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.

Dell Networking OS does not support sending DNS queries over a VLAN. DNS queries are sent out 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.

Syntax `ip domain-name name`

To remove the domain name, use the `no ip domain-name` command.

Parameters

name	Enter one domain name to be used 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
9.7(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.
8.1.1.0	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

Specify the address of a DHCP server so that DHCP broadcast messages can be forwarded when the DHCP server is not on the same subnet as the client.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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.

Dell Networking OS 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 Dell Networking OS forwards to the client with source port=67, destination port=68.



ip helper-address hop-count disable

Disable the hop-count increment for the DHCP relay agent.

Syntax	<pre>ip helper-address hop-count disable</pre> To re-enable the hop-count increment, use the <code>no ip helper-address hop-count disable</code> command.																				
Defaults	Enabled; the hops field in the DHCP message header is incremented by default.																				
Command Modes	CONFIGURATION																				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.3.1.0</td><td>Introduced for the E-Series.</td></tr></tbody></table>	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.	8.1.1.0	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.
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.																				
8.1.1.0	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 incrementing of the hops field when boot requests are relayed to a DHCP server through Dell Networking OS. 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 an IP address to the host-to-IP address mapping table.

Syntax	<pre>ip host name ip-address</pre>



To remove an IP host, use the `no ip host name [ip-address]` command.

Parameters	<i>name</i>	Enter a text string to associate with one IP address.
	<i>ip address</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced for the E-Series.

ip icmp source-interface

Enable the ICMP error and unreachable messages to be sent with the source interface IP address, such as the loopback address, instead of the hops of the preceding devices along the network path to be used for easy debugging and diagnosis of network disconnections and reachability problems with IPv4 packets.

Syntax `ip icmp source-interface interface`

Parameters

<i>interface</i>	Enter one of the following keywords and slot/port[/subport] or number information:

- For a Management Ethernet interface, enter the keyword `managementethernet`.



NOTE: When you configure the capability to enable the loopback IP address to be sent for easy debugging and diagnosis (IP addresses of the devices for which the ICMP source interface is configured), the source IP address of the outgoing ICMP error message is modified, although the packets are not sent out using the configured interface. Because the management interface is configured without any parameters such as the IP address, it is treated to the management interface of the primary unit or the existing unit.

- 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 VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000 platforms.

Usage Information

You can enable the mechanism to configure the source or the originating interface from which the packet (the device that generates the ICMP error messages) is received by the switch to send the loopback address instead of its source IP address to be used in the ICMP unreachable messages and in the `traceroute` command output. The loopback address must be unique in a particular domain.

In network environments that contain a large number of devices, ranging up to thousands of systems, and with each device configured for equal-cost multipath (ECMP) links, you cannot effectively and optimally use the `traceroute` and `ping` applications to examine the network reachability and identify any broken links for diagnostic purposes. In such cases, if the reply that is obtained from each hop on the network path contains the IP address of the adjacent, neighboring interface from which the packet is received, it is difficult to employ the `ping` and `traceroute` utilities. You can enable the ICMP unreachable messages to contain the loopback address of the source device instead of the previous hop's IP address to be able to easily and quickly identify the device and devices along the path because the DNS server maps the loopback IP address to the hostname and does not translate the IP address of every interface of the switch to the hostname.

Example

```
Dell(conf)#ip icmp source-interface tengigabitethernet 1/1/1
Dell(conf)#
```

ipv6 icmp source-interface

Enable the ICMP error and unreachable messages to be sent with the source interface IP address, such as the loopback address, instead of the hops of the preceding devices along the network path to be used for easy debugging and diagnosis of network disconnections and reachability problems with IPv6 packets.

Syntax `ipv6 icmp source-interface interface`

Parameters

<i>interface</i>	Enter one of the following keywords and slot/port[/subport] or number information:
	• For a Management Ethernet interface, enter the keyword <code>managementethernet</code>.



NOTE: When you configure the capability to enable the loopback IP address to be sent for easy debugging and diagnosis (IP addresses of the devices for which the ICMP source interface is configured), the source IP address of the outgoing ICMP error message is modified, although the packets are not sent out using the configured interface. Because the management interface is configurable only without any parameters such as the IP address, it is treated to the management interface of the primary unit or the existing unit.

- 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 VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000 platforms.

Usage Information

You can enable the mechanism to configure the source or the originating interface from which the packet (the device that generates the ICMP error messages) is received by the switch to send the loopback address instead of its source IP address to be used in the ICMP unreachable messages and in the `traceroute` command output. The loopback address must be unique in a particular domain.

In network environments that contain a large number of devices, ranging up to thousands of systems, and with each device configured for equal-cost multipath (ECMP) links, you cannot effectively and optimally use the `traceroute` and `ping` applications to examine the network reachability and identify any broken links for diagnostic purposes. In such cases, if the reply that is obtained from each hop on the network path contains the IP address of the adjacent, neighboring interface from which the packet is received, it is difficult to employ the `ping` and `traceroute` utilities. You can enable the ICMP unreachable messages to contain the loopback address of the source device instead of the previous hop's IP address to be able to easily and quickly identify the device and devices along the path because the DNS server maps the loopback IP address to the hostname and does not translate the IP address of every interface of the switch to the hostname.

Example

```
Dell(conf)#ipv6 icmp source-interface tengigabitethernet 1/1/1
Dell(conf)#
```



ip max-frag-count

Set the maximum number of fragments allowed in one packet for packet re-assembly.

Syntax	<code>ip max-frag-count count</code> To place no limit on the number of fragments allowed, use the <code>no ip max-frag-count</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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.

Syntax	<code>ip name-server ipv4-address [ipv4-address2...ipv4-address6]</code> To remove a name server, use the <code>no ip name-server ip-address</code> command.	
Parameters	ipv4-address	Enter the IPv4 address, in dotted decimal format, of the name server to be used.



ipv4-address2... (OPTIONAL) Enter up five more IPv4 addresses, in dotted decimal format, of name
ipv4-address6 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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

Usage Information Dell Networking OS 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.

ip proxy-arp

Enable proxy ARP on an interface.

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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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.

Syntax `ip route [vrf vrf-name] ip-address mask {ip-address | interface [ip-address]} [distance] [permanent] [tag tag-value] [vrf vrf-name] [weight weight-value]`

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	Enter one of the following keyword followed by the slot/port[/subport] number: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For the Management interface on the stack-unit, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 1 to 6. The port range is 1. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a Null interface, enter the keyword <code>null</code> then the Null interface number. - For a VLAN interface, enter the keyword <code>vlan</code> 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.

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 <i>ip-address</i>	Enter the keyword <code>interface</code> then the IP address.
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 <code>permanent</code> 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 <i>tag-value</i>	(OPTIONAL) Enter the keyword <code>tag</code> then a number to assign to the route. The range is from 1 to 4294967295.
vrf <i>vrf-name</i>	Enter the keyword <code>vrf</code> 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 <i>weight-value</i>	Enter the keyword <code>weight</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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.



Version	Description
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 paths 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 Dell Networking OS to forward IP packets with source route information in the header.

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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.1.1.0	Introduced on the E-Series.

ip tcp initial-time

Define the wait duration in seconds for the TCP connection to be established. This command is supported on the , , , and platforms.

Syntax	<code>ip tcp initial-time <8-75></code> To restore the default behavior, which causes the wait period to be set as 8 seconds, use the <code>no ip tcp initial-time</code> command.

Parameters	<8-75> Wait duration in seconds for the TCP connection to be established.

Command Modes	CONFIGURATION

Command History	<table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.3(0.0)</td><td>Introduced on the S4810, S4820T, S6000, and Z9000 platforms.</td></tr> </table>	Version	Description	9.7(0.0)	Introduced on the S6000-ON.	9.3(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000 platforms.
Version	Description						
9.7(0.0)	Introduced on the S6000-ON.						
9.3(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000 platforms.						

Usage Information	You can configure the amount of time for which the device must wait before it attempts to establish a TCP connection. Using this capability, you can limit the wait times for TCP connection requests. Upon responding to the initial SYN packet that requests a connection to the router for a specific service (such as SSH or BGP) with a SYN ACK, the router waits for a period of time for the ACK packet to be sent from the requesting host that will establish the TCP connection.



ip unknown-unicast

Enable IPv4 catch-all route.

Syntax	<code>ip unknown-unicast</code> 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 <code>no ip unknown-unicast</code> command.	
Defaults	None	
Parameters	vrf <i>vrf-name</i>	(Optional) Enter the keyword <code>vrf</code> followed by the name of the VRF to enable catch-all routes corresponding to that VRF.
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.4(0.0)	Introduced on the S-Series.
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 <code>no ip unknown-unicast</code> command previously. This will be the default configuration after reload.	

ipv4 unicast-host-route

Enable programming of IPv4 /32 route prefixes in L3 host table.

Syntax	[no] ipv4 unicast-host-route							
Defaults	Disabled by default. By default, all the IPv4 route prefixes are installed only in the LPM table.							
Command Modes	CONFIGURATION							
Command History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.3(0.1)</td><td>Introduced on the S6000.</td></tr></table>		Version	Description	9.7(0.0)	Introduced on the S6000-ON.	9.3(0.1)	Introduced on the S6000.
Version	Description							
9.7(0.0)	Introduced on the S6000-ON.							
9.3(0.1)	Introduced on the S6000.							
Usage Information	A warning message is displayed when you enter this command stating that this setting takes effect for existing routes only when IPv4 route prefixes are cleared from the routing table (RTM). To disable this functionality, use no ipv4 unicast-host-route command.							
Example	Dell(conf)#ip unicast-host-route Warning: Command will take effect for existing routes only when IPv4							



```
route prefixes are cleared from RTM
Dell(config)#no ip unicast-host-route
```

show ip tcp initial-time

Displays the interval that you configured for the device to wait before the TCP connection is attempted to be established.

Syntax `show ip tcp initial-time`

Command Modes EXEC

EXEC Privilege

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL platforms.

ip unreachable

Enable the generation of internet control message protocol (ICMP) unreachable messages.

Syntax `ip unreachable`

To disable the generation of ICMP messages, use the `no ip unreachable` 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
9.7(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.
8.1.1.0	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.
pre-6.1.1.0	Introduced on the E-Series.

load-balance

By default, for C-Series and S-Series, Dell Networking OS 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.

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: <code>dest-ip</code> — 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. <code>source-ip</code> — 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: <code>dest-mac</code> — 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. <code>source-dest-mac</code> — 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. <code>source-mac</code> — 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: <code>enable</code> — 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: <code>enable</code> — 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.0	Added the <code>ingress-port</code> 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, Dell Networking OS 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

load-balance hg

Choose the traffic flow parameters the hash calculation uses while distributing the traffic across internal hlgig links.

Syntax	<code>[no] load-balance hg {ip-selection ipv6-selection [source-ip source-ipv6 source-port-id source-module-id dest-ip dest-ipv6 dest-port-id dest-module-id protocol vlan L4-source-port L4-dest-port] mac [source-mac source-port-id source-module-id dest-mac dest-port-id dest-module-id vlan ethertype source-dest-mac] tunnel [ipv4-over-ipv4 ipv4-over-gre-ipv4 mac-in-mac]}</code>

Parameters	{{ip-selection ipv6-selection [source-ip source-ipv6 source-port-id source-module-id dest-ip dest-ipv6 dest-port-id dest-module-id protocol vlan L4-source- To use IPv4 key fields in hash computation, enter the keyword <code>ip-selection</code> then one of the parameters. To use IPv6 key fields in hash computation, enter the keyword <code>ipv6-selection</code> then one of the parameters. • <code>source-ip</code> — Use IPv4 src-ip field in hash calculation. • <code>source-ipv6</code> — Use IPv6 src-ip field in hash calculation • <code>source-port-id</code> — Use src-port-id field in hash calculation. • <code>source-module-id</code> — Use src-module-id field in hash calculation. • <code>dest-ip</code> — Use IPv4 dest-ip field in hash calculation. • <code>dest-ipv6</code> — Use IPv6 dest-ip field in hash calculation



port | L4-dest-port]

- dest-port-id — Use dest-port-id field in hash calculation.
- dest-module-id — Use dest-module-id field in hash calculation.
- protocol — Use IPv4 protocol field in hash calculation.
- vlan — Use vlan field in hash calculation.
- L4-source-port — Use IPv4 L4-source-port field in hash calculation.
- L4-dest-port — Use IPv4 L4-dest-port field in hash calculation.

mac [source-mac | source-port-id | source-module-id | dest-mac | dest-port-id | dest-module-id | vlan | ethertype | source-dest-mac]

To use MAC key fields in hash computation, enter the keyword `mac` then one of the parameters:

- source-mac — Use source-mac field in hash calculation.
- source-port-id — Use src-port-id field in hash calculation.
- source-module-id — Use src-module-id field in hash calculation.
- dest-mac — Use dest-mac field in hash calculation.
- dest-port-id — Use dest-port-id field in hash calculation.
- dest-module-id — Use dest-module-id field in hash calculation.
- vlan — Use vlan field in hash calculation .
- ethertype — Use Ethertype field in hash calculation.
- source-dest-mac — Use SMAC and DMAC fields in hash calculation.

tunnel [ipv4-over-ipv4 | ipv4-over-gre-ipv4 | mac-in-mac]]

To use tunnel key fields in hash computation, enter the keyword `tunnel` then one of the parameters:

- ipv4-over-ipv4 — Use ipv4-over-ipv4 field in hash calculation.
- ipv4-over-gre-ipv4 — Use ipv4-over-gre-ipv4 field in hash calculation.
- mac-in-mac — Use mac-in-mac field in hash calculation.

Defaults

IP selection 5-tuples (source-ip dest-ip vlan protocol L4-source-port L4-dest-port).

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.
9.0.2.0	Introduced on the S6000.
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.



management route

Configure a static route that points to the Management interface or a forwarding router.

Syntax

```
management route {{ip-address mask | {ipv6-address prefix-length}}
{forwarding-router-address | managementethernet | fortyGigE | vlan |
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

<i>ip-address mask</i>	Enter an IP address (dotted decimal format) and mask (/prefix format) of the destination subnet.
<i>ipv6-address prefix-length</i>	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.	
<i>forwarding-router-address</i>	Enter an IP address (dotted decimal format) or an IPv6 address (x:x:x:x::x format) of a forwarding router.
<i>managementethernet</i>	Enter the keyword <code>managementethernet</code> for the Management interface on the Primary RPM.
<i>fortyGigE</i>	Enter the keyword <code>fortyGigE</code> to specify a forty Gigbit Ethernet interface.
<i>vlan</i>	Enter the keyword <code>vlan</code> to specify a vlan interface.
<i>tengigabitethernet</i>	Enter the keyword <code>tengigabitethernet</code> to specify a ten Gigabit Ethernet 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
9.7(0.0)	Added support for forty gigabit, vlan, and tengigabit ethernet interfaces. Introduced on the S6000-ON.
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.



Version	Description
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.

Syntax	<code>show arp [vrf <i>vrf-name</i>] [interface <i>interface</i> ip <i>ip-address</i> [<i>mask</i>] macaddress <i>mac-address</i> [<i>mac-address mask</i>]] [retries] [static dynamic] [inspection {database statistics}] [summary]</code>

Parameters	vrf <i>vrf-name</i> (OPTIONAL) Enter the keyword <code>vrf</code> and then the name of the VRF.  NOTE: Use this attribute to start a BGP instance for either a specific address family corresponding to the default VRF or an IPv4 address family corresponding to a non-default VRF. interface <i>interface</i> (OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For the Management interface on the stack-unit, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 1 to 6. The port range is 1. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094. ip <i>ip-address mask</i> (OPTIONAL) Enter the keyword <code>ip</code> then an IP address in the dotted decimal format. Enter the optional IP address mask in the slash prefix format (<code>/ x</code>). inspection Enter the keyword <code>inspection</code> with one of the following keywords to view ARP entries: <code>database</code> — view a list of ARP entries learned using DAI <code>statistics</code> — view DAI statistics

macaddress mac-address mask	(OPTIONAL) Enter the keyword <code>macaddress</code> then a MAC address in nn:nn:nn:nn:nn:nn format. Enter the optional MAC address mask in nn:nn:nn:nn:nn format also.
static	(OPTIONAL) Enter the keyword <code>static</code> to view entries entered manually.
retries	(OPTIONAL) Enter the keyword <code>retries</code> to show the number of ARP retries before a 20-second back off.
dynamic	(OPTIONAL) Enter the keyword <code>dynamic</code> to view dynamic entries.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view a summary of ARP 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
9.7(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.
8.5.1.0	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).
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 The following example shows two VLANs that are associated with a private VLAN (PVLAN) (refer to [Private VLAN \(PVLAN\)](#)).

If you have entered the `clear arp-cache` command to remove a large number of ARP entries and the command is still being processed in the background, an error message display if you attempt to enter the `show arp` command:

```
Clear arp in-progress. Please try after sometime!
```

The following describes the `show arp` command shown in the following example.

Description

Protocol	Displays the protocol type.
Address	Displays the IP address of the ARP entry.



Description

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 2/13/1 - CP
Internet 192.2.1.253 1 00:00:c0:02:01:02 Te 2/13/2 - CP
Internet 192.2.1.252 1 00:00:c0:02:01:02 Te 2/13/3 - CP
Internet 192.2.1.251 1 00:00:c0:02:01:02 Te 2/13/4 - CP
Internet 192.2.1.250 1 00:00:c0:02:01:02 Te 2/14/1 - CP
Internet 192.2.1.251 1 00:00:c0:02:01:02 Te 2/14/2 - CP
Internet 192.2.1.250 1 00:00:c0:02:01:02 Te 2/14/3 - CP
Internet 192.2.1.249 1 00:00:c0:02:01:02 Te 2/14/4 - CP
Internet 192.2.1.248 1 00:00:c0:02:01:02 Te 2/15/1 - CP
Internet 192.2.1.247 1 00:00:c0:02:01:02 Te 2/15/2 - CP
Internet 192.2.1.246 1 00:00:c0:02:01:02 Te 2/15/3 - CP
Internet 192.2.1.245 1 00:00:c0:02:01:02 Te 2/15/4 - 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 1/1 - CP
Internet 10.10.10.4 1 00:01:e8:d5:9e:e2 Ma 1/1 - CP
Internet 10.16.127.53 1 00:01:e8:d5:9e:e2 Ma 1/1 - CP
Internet 10.16.134.254 20 00:01:e8:d5:9e:e2 Ma 1/1 - CP
Internet 133.33.33.4 1 00:01:e8:d5:9e:e2 Ma 1/1 - CP
```

Usage Information

The following describes the `show arp summary` command shown in the following example.

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.

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
9.7(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.
8.3.1.0	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.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
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.
pre-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: • 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 stack-unit

Display CAM entries for a port-pipe of a stack-unit on a S-Series or Z-Series switch.

Syntax

```
show ip cam stack-unit {stack-unit-number} [port-set {pipe-number} {ip-address mask
[longer-prefixes [ecmp-group detail]]}]| ecmp-group {detail | member-info [detail [gr
index index-number]]}]| summary]
```

Parameters

stack-unit-number	Enter the stack-unit ID. The unit ID range is from 1 to 6.
port-set pipe-number	Enter the keyword <code>port-set</code> then the number of the stack unit's port-pipe. The unit ID range is to 0.
network mask [longer-prefixes [ecmp-group detail]]	(OPTIONAL) Enter the IP address and mask of a route to CAM entries for that route only. You can use one of the following keywords to filter results. • Enter the keyword <code>longer-prefixes</code> to view routes with a common prefix. • Enter the keyword <code>ecmp-group detail</code> to view the ECMP group index.
ecmp-group {detail member-info [detail [group-index index-number]]}	(OPTIONAL) Enter the keyword <code>ecmp-group</code> then one of the following keywords to filter results. • Enter the keyword <code>detail</code> to view the ECMP group index. • Enter the keyword <code>member-info</code> to view the member information for the ECMP group. • Enter the keyword <code>member-info detail</code> to view detailed ECMP membership and n-hop information. • Enter the keyword <code>group-index</code> then the index number to show ECMP membership per group. The range is from 0 to 1022.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view a table listing route prefixes and the total number of routes which can be entered in to CAM.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
7.7.1.0	Added support for up to seven stack members.
7.6.1.0	Introduced on the S-Series.

Usage Information The following describes the `show ip cam` command shown in the following example.

Field	Description
Destination	Displays the destination route of the index.
EC	Displays 1 if the route is an ECMP route. Else, displays 0.
C	This is the CPU bit. If it displays 1, then it indicates that a packet hitting this entry will be forwarded to the CPU.
V Id	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. • CP = control processor • Gi = Gigabit Ethernet interface • Te = 10-Gigabit Ethernet interface

Example

```
Dell#show ip cam stack-unit 3 po 0 1.1.1.0/24 longer-prefixes
```

Destination	EC	C	VId	Mac-Addr	Port
1.1.1.2/32	0	0	3000	00:05:00:00:00:02	Te 3/14/1
1.1.1.1/32	0	1	0	00:00:00:00:00:00	CP
1.1.1.0/24	0	1	0	00:00:00:00:00:00	CP

Dell#

Example (ECMP-Group)

```
Dell#show ip cam stack-unit 3 po 0 ecmp-group detail
```

Destination	EC	C	VId	Mac-Addr	Port	ECMP Group
1.1.1.2/32	0	0	1000	00:01:00:00:00:02	Te 3/12/1	-
2.1.1.2/32	0	0	20	00:03:00:00:00:02	Po 10	-
2.1.1.1/32	0	1	0	00:00:00:00:00:00	CP	-
1.1.1.1/32	0	1	0	00:00:00:00:00:00	CP	-
2.1.1.0/24	0	1	0	00:00:00:00:00:00	CP	-
1.1.1.0/24	0	1	0	00:00:00:00:00:00	CP	-
100.1.1.0/24	1	0	20	00:03:00:00:00:02	Po 10	0
100.1.1.0/24	1	0	1000	00:01:00:00:00:02	Te 3/12/1	0
0.0.0.0/0	0	1	0	00:00:00:00:00:00	CP	-

Dell#

Example (Member-Info)

```
Dell#show ip cam stack-unit 3 po 0 ecmp-group member-info detail
```

Group	Index	Member Count	Mac-Addr	Port	Vlan ID
0		2	00:03:00:00:00:02	Po 10	20
			00:01:00:00:00:02	Te 3/12/1	1000

Dell#



show ip fib stack-unit

View all Forwarding Information Base (FIB) entries of a specific stack-unit.

Syntax	<code>show ip fib stack-unit id vrf vrf-name [ip-address [mask] [longer-prefixes] summary</code>	
Parameters	<i>id</i>	Enter the S-Series stack unit ID. The unit ID range is from 1 to 6.
	<i>vrf vrf-name</i>	Enter the keyword <code>vrf</code> followed by the name of the VRF to view FIB entries corresponding to the VRF.
	<i>ip-address mask</i>	(OPTIONAL) Enter the IP address of the network destination to view only information on that destination. Enter the IP address in dotted decimal format (A.B.C.D). Enter the mask in slash prefix format (/X).
	<i>longer-prefixes</i>	(OPTIONAL) Enter the keywords <code>longer-prefixes</code> to view all routes with a common prefix.
	<i>summary</i>	(OPTIONAL) Enter the keyword <code>summary</code> to view the total number of prefixes in the FIB.

Command Modes	- EXEC - EXEC Privilege

Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS</i> command history. 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.
9.0.2.0	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 up to seven stack members.
7.6.1.0	Introduced on the S-Series.

Usage Information	The following describes the <code>show ip fib stack-unit</code> command shown in the following example.

Field	Description
Destination	Lists the destination IP address.
Gateway	Displays either the word “direct” and an interface for a directly connected route or the remote IP address for a remote route. Traffic is sent to the remote IP address.
First-Hop	Displays the first hop IP address.
Mac-Addr	Displays the MAC address.
Port	Displays the egress-port information.
Vld	Displays the VLAN ID. If no VLAN is assigned, zero (0) is listed.
EC	Displays the number of ECMP paths.



If weighted ECMP is enabled, then the `show ip fib stack-unit` command display a new column named W-EC (W displays either a value of 1 or 0 depending on whether or not a route is assigned with a weight).

Example

```
Dell#show ip fib stack-unit 1
Destination      Gateway          First-Hop      Mac-Addr          Port          Vid
-----
1.1.1.2/32       via 1.1.1.2, V1 1000 1.1.1.2        00:01:00:00:00:02 Te 3/12/1      1000
2.1.1.2/32       via 2.1.1.2, V1 20 2.1.1.2        00:03:00:00:00:02 Po 10          20
0.0.0.0/0        -                0.0.0.0        00:00:00:00:00:00 CP              0
1.1.1.0/24       Direct, V1 1000 0.0.0.0        00:00:00:00:00:00 CP              1000
1.1.1.1/32       via 127.0.0.1    127.0.0.1      00:00:00:00:00:00 CP              0
2.1.1.0/24       Direct, V1 20 0.0.0.0        00:00:00:00:00:00 CP              20
2.1.1.1/32       via 127.0.0.1    127.0.0.1      00:00:00:00:00:00 CP              0
100.1.1.0/24     via 1.1.1.2, V1 1000 1.1.1.2        00:01:00:00:00:02 Te 3/12/1      1000
100.1.1.0/24     via 2.1.1.2, V1 20 2.1.1.2        00:03:00:00:00:02 Po 10          20
Dell#

Dell#show ip route
S    10.1.1.0/24      via 1.1.1.2, V1 10
                        via 2.1.1.2, V1 20
S    20.1.1.0/24      via 3.1.1.2, V1 30
S    100.1.1.0/24     via 10.1.1.0, weight 7
                        via 20.1.1.0, weight 1
```

Example (Show command output with Weighted ECMP Enabled)

```
Dell#show ip fib stack-unit 1
Destination      Gateway          First-Hop      Mac-Addr          Port
-----
0.0.0.0/0        -                0.0.0.0        00:00:00:00:00:00 CP
1.1.1.0/24       Direct, Lo 0     0.0.0.0        00:00:00:00:00:00 CP
1.1.1.1/32       via 127.0.0.1    127.0.0.1      00:00:00:00:00:00 CP
```

The RC and W columns in the show output appear only if the weighted ECMP is enabled using the `ip ecmp weighted`.

Related Commands [clear ip fib stack-unit](#) — clear FIB entries on a specified stack-unit.

[ip ecmp weighted](#) — enables weighted ECMP calculations.

show ip flow

Show how a Layer 3 packet is forwarded when it arrives at a particular interface.

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/subport 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 <i>destination-ip</i> then the IP destination address in IP address format.
protocol number [tcp udp]	Enter the keyword <i>protocol</i> then one of the protocol type keywords: <i>tcp</i> , <i>udp</i> , or <i>protocol number</i> . The protocol number range is from 0 to 255. .
src-port number	Enter the keywords <i>src-port</i> then the source port number.
destination-port number	Enter the keywords <i>destination-port</i> then the destination port 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
9.7(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.
8.3.10.0	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.
pre-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 packets 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 2/42/1 20.1.1.1 100.1.1.2 protocol tcp
Flow: 20.1.1.1 100.1.1.2 6
Ingress interface: Te 2/42/1
Egress Interface: Te 2/43/1
Dell#
```



show ip interface

View IP-related information on all interfaces.

Syntax `show ip interface [interface | brief] [configured]`

Parameters

<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For the Management interface on the stack-unit, enter the keyword <code>ManagementEthernet</code> then the slot/port information. The slot range is from 1 to 6. The port range is 1. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a Null interface, enter the keyword <code>null</code> then the Null interface number. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094. • For a stack-unit interface, enter the keyword <code>stack-unit</code> then the stack unit number. • For a tunnel interface, enter the keyword <code>tunnel</code> then the tunnel interface number. The range is from 1 to 16383.
<i>brief</i>	(OPTIONAL) Enter the keyword <code>brief</code> to view a brief summary of the interfaces and whether an IP address is assigned.
<i>configured</i>	(OPTIONAL) Enter the keyword <code>configured</code> 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
9.7(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.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.



Version	Description
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.
pre-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 1/1...	Displays the interface's type, slot/port/subport, 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 unreachable...	States if ICMP unreachable messages are sent.

Example

```

Dell#show ip int te 1/1/1
TenGigabitEthernet 1/1/1 is down, line protocol is down
Internet address is not set
IP MTU is 1500 bytes
Inbound access list is not set
Proxy ARP is enabled
Split Horizon is enabled
Poison Reverse is disabled
ICMP redirects are not sent
ICMP unreachables are not sent

Dell#

```

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 interface brief
Interface          IP-Address  OK? Method  Status
Protocol
TenGigabitEthernet 1/1/1      unassigned NO  Manual    administratively down
down
TenGigabitEthernet 1/1/2      unassigned NO  Manual    administratively down
down
TenGigabitEthernet 1/1/3      unassigned YES Manual    up
TenGigabitEthernet 1/1/4      unassigned YES Manual    up
TenGigabitEthernet 1/2/1      unassigned YES Manual    up
TenGigabitEthernet 1/2/2      10.10.10.1 YES Manual    up
TenGigabitEthernet 1/2/3      unassigned NO  Manual    administratively down
down
```

show ip management-route

View the IP addresses assigned to the Management interface.

Syntax

```
show ip management-route [all | connected | summary | static]
```

Parameters

all	(OPTIONAL) Enter the keyword <code>all</code> to view all IP addresses assigned to all Management interfaces on the switch.
connected	(OPTIONAL) Enter the keyword <code>connected</code> to view only routes directly connected to the Management interface.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view a table listing the number of active and non-active routes and their sources.
static	(OPTIONAL) Enter the keyword <code>static</code> 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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
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 management-route

Destination      Gateway          State
-----
10.1.2.0/24      ManagementEthernet 1/1  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.

Syntax `show ipv6 management-route [all | connected | summary | static]`

Parameters

all	(OPTIONAL) Enter the keyword <code>all</code> to view all IP addresses assigned to all Management interfaces on the switch.
connected	(OPTIONAL) Enter the keyword <code>connected</code> to view only routes directly connected to the Management interface.
summary	(OPTIONAL) Enter the keyword <code>summary</code> to view a table listing the number of active and non-active routes and their sources.
static	(OPTIONAL) Enter the keyword <code>static</code> to view non-active routes also.

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
9.7(0.0)	Introduced on the S6000-ON.
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 1/1  Connected
```



2001:68::0/64
Dell#

2001:34::16

Active

show ip protocols

View information on all routing protocols enabled and active on the switch.

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
97(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.
8.1.1.0	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.
pre-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.

Syntax

```
show ip route [vrf vrf-name] hostname | ip-address [mask] [longer-prefixes] |  
list prefix-list | protocol [process-id | routing-tag] | all | connected |  
static | summary]
```

Parameters

<i>vrf vrf-name</i>	(OPTIONAL) Enter the keyword <code>vrf</code> and then the VRF name to list the routes in the route table of a specific VRF.
<i>ip-address</i>	(OPTIONAL) Specify a name of a device or the IP address of the device to view more detailed information about the route.
<i>mask</i>	(OPTIONAL) Specify the network mask of the route. Use this parameter with the IP address parameter.
<i>longer-prefixes</i>	(OPTIONAL) Enter the keywords <code>longer-prefixes</code> to view all routes with a common prefix.
<i>list prefix-list</i>	(OPTIONAL) Enter the keyword <code>list</code> and the name of a configured prefix list. For more information, refer to the show ip route list command.
<i>protocol</i>	(OPTIONAL) Enter the name of a routing protocol (<code>bgp</code> , <code>isis</code> , <code>ospf</code> , <code>rip</code>) or the keywords <code>connected</code> or <code>static</code> .



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*.

<i>process-id</i>	(OPTIONAL) Specify that only OSPF routes with a certain process ID must be displayed.
<i>routing-tag</i>	(OPTIONAL) Specify that only ISIS routes with a certain routing tag must be displayed.
<i>connected</i>	(OPTIONAL) Enter the keyword <code>connected</code> to view only the directly connected routes.
<i>all</i>	(OPTIONAL) Enter the keyword <code>all</code> to view both active and non-active routes.
<i>static</i>	(OPTIONAL) Enter the keyword <code>static</code> to view only routes the <code>ip route</code> command configures.
<i>summary</i>	(OPTIONAL) Enter the keyword <code>summary</code> . 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
9.7(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.
8.1.1.0	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 The following describes the `show ip route all` command in the following example.

Field	Description
(undefined)	Identifies the type of route: • 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 IP 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.



Field	Description
Last Change	Identifies when the route was last changed or configured.

The weight for weighted ECMP route calculations is displayed for each path in the route in `show ip route` command. The ECMP weight is displayed only if weighted ECMP is enabled using the `ip ecmp weighted` command is enabled.

If weighted ECMP is disabled, the `show ip route` command does not show the weighted ECMP route information.

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, Te 2/8/1 120/1    00:07:12
      via 101.10.10.10, Te 2/8/2
      100.10.10.0/24    Direct, Te 2/8/2          0/0      00:08:54
> R  100.10.10.0/24    Direct, Te 2/8/4          120/0     00:08:54
C    101.10.10.0/24    Direct, Te 2/9/1          0/0      00:09:15
> R  101.10.10.0/24    Direct, Te 2/9/2          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
R1_E600i>show ip route static ?
|
| Pipe through a command
|
<cr>
R1_E600i>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    1/0        3d2h
Dell>
```

Example (With Weighted ECMP Enabled)

```
Dell(conf)#ip route 1.1.1.0/24 6.6.6.2 weight 100
Dell(conf)#ip route 1.1.1.0/24 6.6.6.2 weight 200
Dell(conf)#do show ip route
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
Metric Last Change      Dist/
```



```

-----
S      1.1.1.0/24      4.4.4.2, via Te 1/4/1 , weight
100                                     1/0      00:00:01
                                     6.6.6.2, via Te 1/16/1, weight 200
C      4.4.4.0/24      Direct, Te
1/4/1                                     0/0
00:01:32
C      6.6.6.0/24      Direct, Te
1/16/1                                     0/0
00:01:25

```

```

Dell# show ip route 1.1.1.0/24
Routing entry for 1.1.1.0/24
  Known via "static", distance 1, metric 0
  Last update 00:05:01 ago
  Routing Descriptor Blocks:
    * 4.4.4.2, via TenGigabitEthernet 1/4/1 weight 100
    * 6.6.6.2, via TenGigabitEthernet 1/16/1 weight 200
Dell(conf)#

```

Example (With Weighted ECMP Disabled)

```

Dell(conf)#ip route 1.1.1.0/24 6.6.6.2 weight 100
Dell(conf)#ip route 1.1.1.0/24 6.6.6.2 weight 200
Dell(conf)#do show ip route
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
Metric Last Change
-----
S      1.1.1.0/24      4.4.4.2, via Te
1/4/1                                     1/0      00:00:01
                                     6.6.6.2, via Te 1/16/1
C      4.4.4.0/24      Direct, Te
1/4/1                                     0/0
00:01:32
C      6.6.6.0/24      Direct, Te
1/16/1                                     0/0
00:01:25

Dell(conf)#do show ip route 1.1.1.0/24
Routing entry for 1.1.1.0/24
  Known via "static", distance 1, metric 0
  Last update 00:05:01 ago
  Routing Descriptor Blocks:
    * 4.4.4.2, via GigabitEthernet 1/4
    * 6.6.6.2, via GigabitEthernet 1/16
Dell(conf)#

```



show ip route list

Display IP routes in an IP prefix list.

Syntax `show ip route vrf vrf-name list prefix-list`

Parameters

prefix-list	Enter the name of a configured prefix list.
vrf vrf-name	Enter the keyword <code>vrf</code> followed by the name of the VRF to display IP routes in an IP prefix list 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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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 4/13/1	120/2	3d0h
R	2.1.1.0/24	via 2.1.4.1, Te 4/13/2	120/2	3d1h
R	2.1.2.0/24	via 2.1.4.1, Te 4/13/3	120/1	3d0h
R	2.1.3.0/24	via 2.1.4.1, Te 4/13/4	120/1	3d1h
C	2.1.4.0/24	Direct, Te 4/14/1	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.

Syntax `show ip route vrf vrf-name 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
9.7(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.
8.1.1.0	Introduced on the E-Series ExaScale.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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 Dell Networking OS.
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.



Column Heading	Description

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 Dell Networking OS, 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, ICMP, UDP, TCP and ARP traffic statistics.

Syntax

```
show ip traffic [all | cp | rp1 | rp2]
```



NOTE: These options are supported only on the E-Series.

Parameters

all	(OPTIONAL) Enter the keyword <code>all</code> to view statistics from all processors. If you do not enter a keyword, you also view all statistics from all processors.
cp	(OPTIONAL) Enter the keyword <code>cp</code> to view only statistics from the Control Processor.
rp1	(OPTIONAL) Enter the keyword <code>rp1</code> to view only the statistics from Route Processor 1.
rp2	(OPTIONAL) Enter the keyword <code>rp2</code> to view only the statistics from Route Processor 2.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
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	F10 Monitoring MIB available for the <code>ip traffic statistics</code> command.
pre-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 Dell Networking OS.
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 - destination IP address belongs to reserved prefixes; the host/network is unreachable
bad options...	Unrecognized IP option on a received packet.
Frag:	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. Dell Networking OS sends an arp request prior to forwarding an IP packet. If a reply is not received, Dell Networking OS repeats the request three times. These packets are counted in encapsulation failed.
Rcvd:	
...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 Dell 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)
Routing Processor1 IP Traffic:
```

show tcp statistics

View information on TCP traffic through the switch.

Syntax

```
show tcp statistics {all | cp | rp1 | rp2}
```

Parameters

all	Enter the keyword all to view all TCP information.
cp	Enter the keyword cp to view only TCP information from the Control Processor.
rp1	Enter the keyword rp1 to view only TCP statistics from Route Processor 1.
rp2	Enter the keyword rp2 to view only TCP statistics from Route Processor 2.



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.

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.
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. • 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.



Field	Description
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 stat 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 [show ip cam stack-unit](#) — displays the CAM table.



IPv6 Basics

IPv6 basic commands are supported on the Dell Networking OS.

 **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*.

cam-ipv6 extended-prefix

Enable LPM partitioning to support IPv6 /65 to /128 route prefixes to be stored in Partition 1.

Syntax	cam-ipv6 extended-prefix <Max-IPv6-prefixes>	
	To remove LPM partitioning configuration, use no cam-ipv6 extended-prefix.	
Parameters	Max-IPv6-Prefix	Maximum number of IPv6 prefixes in the mask length of /65 to /128. The possible values are 1024, 2048, and 3072.
Defaults	LPM is not partitioned with Partition 1 and therefore /65 to /128 prefixes are not converted to /64 prefixes and are installed and saved in LPM. All the packets for those routes traverse through the default route path.	
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.3(0.1)	Introduced on the S6000.
Usage Information	You can partition the LPM table to store IPv6 prefixes greater than /64 mask length. Requires reboot of the switch to take effect as the SDK handles this only during its initialization.	

clear ipv6 route

Clear (refresh) all or a specific route from the IPv6 routing table.

Syntax	clear ipv6 route [vrf vrf-name] {* ipv6-address prefix-length}

Parameters

<code>vrf vrf-name</code>	(Optional) Enter the keyword <code>vrf</code> followed by the name of the VRF to clear the IPv6 routes corresponding to that VRF.
<code>*</code>	Enter the <code>*</code> to clear (refresh) all routes from the IPv6 routing table.
<code>ipv6-address prefix-length</code>	Enter the IPv6 address in the <code>x::x::x</code> format then the prefix length in the <code>/x</code> format. The range is from <code>/0</code> to <code>/128</code> .



NOTE: The `::` notation specifies successive hexadecimal fields of zeros.

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
9.7(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.

maximum dynamic-routes-ipv6

Specify the maximum number of dynamic (protocol) IPv6 routes a VRF can have.

Syntax

```
maximum dynamic-routes-ipv6 limit {warn-threshold threshold-value | warning-only}
```

To remove the limit on the maximum number of IPv6 routes used, use the `no maximum dynamic-routes-ipv6` command.

Parameters

<code>limit</code>	Maximum number of IPv6 routes allowed in a VRF. Valid range is from 1 to 8000 (or maximum allowable for that platform if smaller value).
<code>warning-threshold</code>	Warning threshold value is expressed as a percentage of the limit value. When the number of IPv6 routes reaches the specified percentage of the limit, a warning message is generated. Valid range is 1 to 100. When <code>warn-threshold</code> is used, once the limit is reached, additional routes will not be allowed into the RTM (route table manager) itself.



warning-only When the warning-only option is used, a syslog message will be thrown when maximum number of dynamic IPv6 routes reaches the limit. Additional dynamic IPv6 routes will still be allowed.

Defaults No limit is set on the maximum number of dynamic IPv6 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 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 S4810, S4820T, S5000, S6000, S6000-ON, and Z9500.

Usage Information If the maximum IPv6 route limit is not specified for a VRF (valid range is from 1 to 8000), 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 cam-ipv6 extended-prefix

Display the current settings and next-boot settings for cam-ipv6 extended-prefix configuration. Display the cam-ipv6 extended-prefix configuration.

Syntax `show cam-ipv6 extended-prefix`

Defaults None

Command Modes EXEC
EXEC Privilege

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.1)	Introduced on the S6000.

Usage Information You can use this command to view the number of supported extended prefix entries in LPM configured. The output also displays the current applied value and the new value that is applicable after the reboot of the device.

Example

```
Dell# show cam-ipv6 extended-prefix
Cam-Ipv6-LPM Extended Prefix
-----
Current Settings
cam-ipv6-max-/65-to-/128-Prefix : 2048
Dell(conf) #
```



ipv6 unicast-host-route

Enable programming of IPv6 /128 route prefixes in L3 host table.

Syntax	[no] ipv6 unicast-host-route	
Defaults	Enabled by default. By default, all the IPv6/128 route prefixes are installed only in L3 host table.	
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.3(0.1)	Introduced on the S6000.
Usage Information	You can use this command to enable programming of /128 route prefixes in L3 host table or in LPM table. A warning message is displayed when you enter this command stating that this setting takes effect for existing routes only when IPv6 route prefixes are cleared from the routing table (RTM). To enable programming of /128 route prefixes in LPM table, use no ipv6 unicast-host-route command.	
Example	<pre>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)#</pre>	

ipv6 nd dns-server

Configures Recursive DNS Server (RDNSS) addresses to be distributed via IPv6 router advertisements to an IPv6 device.

Syntax	<pre>ipv6 nd dns-server {ipv6-RDNSS-address} {lifetime infinite}</pre> 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 CONFIG	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000–ON.
	9.5(0.0)	Introduced on the Z9000, S6000, S4810, S4820T, and MXL..
Usage Information	Use this 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.	
Example	<pre>Dell(conf-if-te-1/1/1)#ipv6 nd dns-server 1000::1 1</pre>	

ipv6 route

Establish a static IPv6 route.

Syntax	<pre>ipv6 route [vrf vrf-name] ipv6-address prefix-length {ipv6-address interface interface ipv6-address} [distance] [tag value] [permanent] [weight weight-value]</pre> To remove the IPv6 route, use the <code>no ipv6 route [vrf vrf-name] ipv6-address prefix-length {ipv6-address interface interface ipv6-address} [distance] [tag value] [permanent] [weight]</code> command.

Parameters	vrf vrf-name	(Optional) Enter the keyword <code>vrf</code> followed by the name of the VRF to install IPv6 routes in that VRF.
	ipv6-address prefix-length	Enter the IPv6 address in the <code>x::x::x::x</code> format then the prefix length in the <code>/x</code> format. The range is from <code>/0</code> to <code>/128</code> .
	interface	(OPTIONAL) Enter the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a Null interface, enter the keyword <code>null</code> then the Null interface number. - For a tunnel interface, enter the keyword <code>tunnel</code> then the tunnel interface number. The range is from 1 to 16383. - For a VLAN interface, enter the keyword <code>VLAN</code> then the vlan number. The range is from 1 to 4094.



NOTE: The `::` notation specifies successive hexadecimal fields of zeros.

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.

<i>ipv6-address</i>	(OPTIONAL) Enter the forwarding router IPv6 address in the x:x:x:x format.  NOTE: The :: notation specifies successive hexadecimal fields of zeros.
<i>distance</i>	(OPTIONAL) Enter a number as the metric distance assigned to the route. The range is from 1 to 255.
<i>tag value</i>	(OPTIONAL) Enter the keyword <code>tag</code> then a tag value number. The range is from 1 to 4294967295.
<i>permanent</i>	(OPTIONAL) Enter the keyword <code>permanent</code> 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 <code>permanent</code>, the route disappears from the routing table.
<i>weight weight-value</i>	Enter the keyword <code>weight</code> 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 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
9.7(0.0)	Added support for VRF. Also included the <code>weight</code> 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.

show ipv6 route

Displays the IPv6 routes.

Syntax

```
show ipv6 route [ipv6-address prefix-length] [vrf vrf-name] [hostname]
[all] [bgp as number] [connected] [isis tag] [list prefix-list name] [ospf
process-id] [rip] [static] [summary]
```

Parameters

ipv6-address prefix-length (OPTIONAL) Enter the IPv6 address in the 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 followed by 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.

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.

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
9.7(0.0)	Added support for VRF. Introduced on 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.
8.2.1.0	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: • 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



Field	Description
	· + = 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 (S-Series)

```
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      100::/64 [0/0]
          Direct, Gi 1/12, 20:00:18
C      400::/64 [0/0]
          Direct, Tu 1, 00:09:02
S      800::/64 [1/0]
          via 100::1, Gi 1/12, 00:00:50
L      fe80::/10 [0/0]
          Direct, Nu 0, 20:00:18
Dell#

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      100::/64 [0/0]
          Direct, Te 1/12, 20:00:18
C      400::/64 [0/0]
          Direct, Tu 1, 00:09:02
S      800::/64 [1/0]
          via 100::1, Te 1/12, 00:00:50
L      fe80::/10 [0/0]
          Direct, Nu 0, 20:00:18
Dell#
```

Example (Summary)

```
show ipv6 route summary:
=====
Dell#show ipv6 route summary

Route Source      Active Routes  Non-active Routes
connected         3              0
static            1              0
Total             4              0
```



```
Total 4 active route(s) using 928 bytes
Dell#
```



IPv6 Access Control Lists (IPv6 ACLs)

IPv6 ACLs and IPv6 Route Map commands are supported on Dell Networking platform.

 **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, refer to 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.

show cam-acl-egress

Show information on FP groups allocated for egress ACLs.

Syntax `show cam-acl-egress`

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.



Version	Description
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.
8.4.2.0	Introduced on the E-Series TeraScale.
7.8.1.0	Introduced on the C-Series.

Example

```
Dell#show cam-acl-egress

-- Chassis Egress Cam ACL --
      Current Settings(in block sizes)
L2Acl   :      1
Ipv4Acl :      1
Ipv6Acl :      2

-- Stack unit 1 --
      Current Settings(in block sizes)
L2Acl   :      1
Ipv4Acl :      1
Ipv6Acl :      2

Dell#show cam-acl
```

Related Commands [cam-acl](#) — configures CAM profiles to support IPv6 ACLs.

show cam-acl

Show space allocated for IPv6 ACLs.

Syntax `show cam-acl`

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.4.2.1	Introduced on the S-Series.
8.4.2.0	Introduced on the E-Series TeraScale.



Version	Description
7.8.1.0	Introduced on the C-Series.

Example

```
show cam-acl (non default)
Dell(conf)#cam-acl l2acl 2 ipv4acl 4 ipv6acl 4 ipv4qos 2 l2qos 1 l2pt 0
ipmacacl 0 vman-qos 0 ecfmacl 0
Dell#show cam-acl

-- Chassis Cam ACL --
      Current Settings(in block sizes)
      1 block = 128 entries
L2Acl      :      2
Ipv4Acl    :      4
Ipv6Acl    :      4
Ipv4Qos    :      2
L2Qos      :      1
L2PT       :      0
IpMacAcl   :      0
VmanQos    :      0
VmanDualQos :      0
EcfmAcl    :      0
FcoeAcl    :      0
iscsiOptAcl :      0
ipv4pbr    :      0
vrfv4Acl   :      0
Openflow   :      0
fedgovacl  :      F3940

-- stack-unit 1 --
      Current Settings(in block sizes)
      1 block = 128 entries
L2Acl      :      2
Ipv4Acl    :      4
Ipv6Acl    :      4
Ipv4Qos    :      2
L2Qos      :      1
L2PT       :      0+F394
IpMacAcl   :      0
VmanQos    :      0
VmanDualQos :      0
EcfmAcl    :      0
FcoeAcl    :      0
iscsiOptAcl :      0
ipv4pbr    :      0
vrfv4Acl   :      0
Openflow   :      0
fedgovacl  :      0

Dell#
```

Example (Manual Profiles)

```
Dell#show cam-acl

-- Chassis Cam ACL --
      Current Settings(in block sizes)
L2Acl      :      2
Ipv4Acl    :      2
Ipv6Acl    :      4
Ipv4Qos    :      2
L2Qos      :      3

-- Line card 4 --
      Current Settings(in block sizes)
L2Acl      :      2
Ipv4Acl    :      2
Ipv6Acl    :      4
Ipv4Qos    :      2
```



```
L2Qos      :          3
Dell#show cam-acl
```

Related Commands [cam-acl](#) — configures CAM profiles to support IPv6 ACLs.

permit icmp

To allow all or specific internet control message protocol (ICMP) messages, configure a filter.

Syntax `permit icmp {source address mask | any | host ipv6-address} {destination address | any | host ipv6-address} [count [byte]]`

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

Defaults Not configured.

Command Modes 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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	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. Added the <code>monitor</code> option.

permit

To configure a filter that matches the filter criteria, select an IPv6 protocol number, ICMP, IPv6, TCP, or UDP.

Syntax `permit {ipv6-protocol-number | icmp | ipv6 | tcp | udp}`



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

<i>ip-protocol-number</i>	Enter an IPv6 protocol number. The range is from 0 to 255.
<i>icmp</i>	Enter the keyword <code>icmp</code> to filter internet Control Message Protocol version 6.
<i>ipv6</i>	Enter the keyword <code>ipv6</code> to filter any internet Protocol version 6.
<i>tcp</i>	Enter the keyword <code>tcp</code> to filter the Transmission Control protocol.
<i>udp</i>	Enter the keyword <code>udp</code> to filter the User Datagram Protocol.

Defaults

Not configured.

Command Modes

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.

ipv6 control-plane egress-filter

Enable egress Layer 3 ACL lookup for IPv6 CPU traffic.

Syntax

`ipv6 control-plane egress-filter`

Defaults

Not enabled.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.3.10.0	Introduced on the S4810.

ipv6 access-list

Configure an access list based on IPv6 addresses or protocols.

Syntax `ipv6 access-list access-list-name cpu-qos {permit | deny} ospfv3`
 To delete an access list, use the `no ipv6 access-list access-list-name` command.

Parameters	<i>access-list-name</i>	Enter the access list name as a string, up to 140 characters.
	cpu-qos	Enter the keyword <code>cpu-qos</code> to assign this ACL to control plane traffic only (CoPP).
	permit	Enter the keyword <code>permit</code> to configure a filter to forward packets meeting this condition.
	deny	Enter the keyword <code>deny</code> to configure a filter to drop packets meeting this condition.
	ospfv3	Specify that this ACL is for OSPFv3 control plane traffic

Defaults All access lists contain an implicit “deny any”; that is, if no match occurs, the packet is dropped.

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.
9.4(0.0)	Added support for CoPP for OSPFv3 on the S4810, S4820T, S6000, and Z9000 platforms.
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.
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.



Version	Description
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. You can create an IPv6 ACL for control-plane traffic policing for OSPFv3, in addition to the CoPP support for VRRP, BGP, and ICMP.

cam-acl-egress

Allocate space for IPv6 egress ACLs.

Syntax `cam-acl-egress {default | l2acl 1-4 ipv4acl 1-4 ipv6acl 0-4}`

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 1-4 ipv4acl 1-4 ipv6acl 0-4 Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the amount to be allotted. The total space allocated must equal 4. The `ipv6acl` range must be a factor of 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
9.7(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.
8.4.2.0	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.

The total amount of space allowed is 4 FP Blocks.



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 ?
<1-4>        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 ?
<0-4>        Number of FP blocks for IPV6 (multiples of 2)
Dell(conf)#cam-acl-egress l2acl 1 ipv4acl 1 ipv6acl 2
```

cam-acl

Allocate space for IPv6 ACLs.

Syntax

```
cam-acl {default | l2acl 1-10 ipv4acl 1-10 ipv6acl 0-10 ipv4qos 1-10 l2qos
1-10}
```

Parameters

default

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

- L3 ACL (ipv4acl): **6**
- L2 ACL(l2acl): **5**
- IPv6 L3 ACL (ipv6acl): **0**
- L3 QoS (ipv4qos): **1**
- L2 QoS (l2qos): **1**

**l2acl 1-10 ipv4acl
1-10 ipv6acl 0-10
ipv4qos 1-10 l2qos
1-10**

Allocate space to support IPv6 ACLs. Enter all of the profiles and a range. Enter the CAM profile name then the amount to be allotted. The total space allocated must equal 13. The `ipv6acl` range must be a factor of 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
9.7(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.



Version	Description
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.

The total amount of space allowed is 16 FP blocks. System flow requires three blocks and these blocks cannot be reallocated.

When configuring space for IPv6 ACLs, 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).



Intermediate System to Intermediate System (IS-IS)

The intermediate system to intermediate system (IS-IS) protocol for IPv4 and IPv6 is supported on the S6000-ON platform. 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.**

adjacency-check

Verify that the “protocols supported” field of the IS-IS neighbor contains matching values to this router.

Syntax	adjacency-check To disable adjacency check, use the <code>no adjacency-check</code> command.										
Defaults	Enabled.										
Command Modes	- ROUTER ISIS (<i>for IPv4</i>) - CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> </table>	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.	8.3.12.0	Introduced on the S4810.
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.										
8.3.12.0	Introduced on the S4810.										



Version	Description
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).

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 <code>level1-into-level2</code> to advertise Level 1 routes into Level 2 LSPs. This setting is the default.
level2-into-level1	Enter the keywords <code>level2-into-level1</code> 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 is enabled.)
level2-into-level1 (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
9.7(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.
8.3.11.1	Introduced on the Z9000.



Version	Description
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 Level 1 to Level 2. Also, you cannot enable leaking from Level 2 to Level 1. 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 Level 1 routes are leaked.

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.

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 <code>hmac-md5</code> to encrypt the password.
<i>encryption-type</i>	(OPTIONAL) Enter 7 to encrypt the password using DES.
<i>password</i>	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
9.7(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.
8.3.11.1	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 config

Clear IS-IS configurations that display under the *router isis* heading of the `show running-config` command output.

Syntax `clear config`

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
9.7(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.
8.3.7.1	Introduced on the S4810.

Usage Information



CAUTION: Use caution when you enter this command. Back up your configuration prior to using this command or your IS-IS configuration will be erased.

clear isis

Restart the IS-IS process. All IS-IS data is cleared.

Syntax `clear isis [vrf vrf-name] [tag] {* | database | traffic}`

Parameters

vrf vrf-name	(Optional) Enter the keyword <code>vrf</code> 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 <code>*</code> 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
9.7(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.
8.3.12.0	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.

Syntax `clns host name nsap`

Parameters

<i>name</i>	Enter an alphanumeric string to identify the name-to-NSAP mapping.
<i>nsap</i>	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
9.7(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.
8.3.11.1	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.

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
9.7(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.
8.3.11.1	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.

Syntax `debug isis [vrf vrf-name] adj-packets [interface]`
To turn off debugging, use the `no debug isis [vrf vrf-name]adj-packets [interface]` command.

Parameters

vrf vrf-name	(Optional) Enter the keyword <code>vrf</code> 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[/subport] as one of the following: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> 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
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
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 local-updates

To debug IS-IS local update packets, enable debugging on a specific interface and provides diagnostic information.

Syntax `debug isis [vrf vrf-name] local-updates [interface]`
 To turn off debugging, use the `no debug isis [vrf vrf-name] updates [interface]` command.

Parameters

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.

interface (OPTIONAL) Identifies the interface type slot/port[/subport] as one of the following:

- 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.
- 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
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
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.

Syntax `debug isis [vrf vrf-name] snp-packets [interface]`
To turn off debugging, use the `no debug isis [vrf vrf-name] snp-packets [interface]` command.

Parameters

vrf vrf-name	(Optional) Enter the keyword <code>vrf</code> 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.
interface	(OPTIONAL) Identifies the interface type slot/port[/subport] as one of the following: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a VLAN interface, enter the keyword <code>vlan</code> 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 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)	Added support for VRF. Introduced on the S6000-ON.
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.

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
9.7(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.
8.3.12.0	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.

Syntax

debug isis [vrf vrf-name] update-packets [interface]

To turn off debugging, use the no debug isis update-packets [interface] command.

Parameters

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.

interface

(OPTIONAL) Identifies the interface type slot/port[/subport] as one of the following:

- 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.

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
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
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.

Syntax	<pre>default-information originate [always] [metric metric] [route-map map-name]</pre>



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 <code>always</code> to have the default route always advertised.
metric <i>metric</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number to assign to the route. The range is from 0 to 16777215.
route-map <i>map-name</i>	(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
9.7(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.
8.3.11.1	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.

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
	9.7(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.
	8.3.11.1	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.

Syntax `distance weight [ip-address mask [prefix-list]]`
To return to the default values, use the `no distance weight` command.

Parameters

<i>weight</i>	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 .
<i>ip-address mask</i>	(OPTIONAL) Enter the next-hop address in dotted decimal format and enter a mask in either dotted decimal or /prefix format.
<i>prefix-list</i>	(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
9.7(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.
8.3.11.1	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.

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

<i>prefix-list-name</i>	Specify the prefix list to filter prefixes in routing updates.
<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port[/subport] as one of the following: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN interface, enter the keyword <code>vlan</code> 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
9.7(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.
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.

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

<i>prefix-list-name</i>	Specify the prefix list to filter prefixes in routing updates.
connected	(OPTIONAL) Enter the keyword <code>connected</code> for directly connected routing process.
ospf <i>process-id</i>	(OPTIONAL) Enter the keyword <code>ospf</code> then the OSPF process-ID number. The range is from 1 to 65535.
bgp <i>as number</i>	(OPTIONAL) Enter the BGP then the AS Number. The range is from 1 to 65535.
rip	(OPTIONAL) Enter the keyword <code>rip</code> for RIP routes.
static	(OPTIONAL) Enter the keyword <code>static</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.
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.

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
9.7(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.
8.3.11.1	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.

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 <code>hmac-md5</code> to encrypt the password using MD5.
<i>encryption-type</i>	(OPTIONAL) Enter 7 to encrypt the password using DES.
<i>password</i>	Enter an alphanumeric string up to 16 characters long. If you do not specify an <code>encryption type</code> or <code>hmac-md5</code> 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
9.7(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.
8.3.11.1	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.

Syntax `graceful-restart ietf`
To return to the default, use the `no graceful-restart ietf` command.

Parameters

ietf	Enter <code>ietf</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

Syntax	<code>graceful-restart interval minutes</code> To return to the default, use the <code>no graceful-restart interval</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.



Version	Description
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.
8.3.1.0	Introduced on the E-Series.

graceful-restart restart-wait

Enable the graceful restart maximum wait time before a restarting peer comes up.

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
9.7(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.
8.3.11.1	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.

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 <code>interval</code> to set the wait time. The range is from 5 to 120 seconds. The default is 5 seconds .
retry-times	Enter the keywords <code>retry-times</code> 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
9.7(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.
8.3.11.1	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.

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 <code>level-1</code> or <code>level-2</code> to identify the database instance type to which the wait interval applies.
seconds	Enter the <code>graceful-restart t2</code> 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
9.7(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.
8.3.11.1	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.

Syntax `graceful-restart t3 {adjacency | manual} seconds`
To return to the default, use the `no graceful-restart t3` command.

Parameters

adjacency	Enter the keyword <code>adjacency</code> 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 <code>manual</code> 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
9.7(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.
8.3.11.1	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 <code>no graceful-restart restart-wait</code> command. When you disable <code>restart-wait</code>, the current adjacency hold time is used. Set the <code>t3</code> timer to <code>adjacency</code> 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 <code>graceful-restart t3 adjacency</code>.
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.

Syntax	<code>hello padding [multi-point point-to-point]</code> To return to the default, use the <code>no hello padding [multi-point point-to-point]</code> command.													
Parameters	multi-point	(OPTIONAL) Enter the keywords <code>multi-point</code> to pad only LAN hello PDUs.												
	point-to-point	(OPTIONAL) Enter the keywords <code>point-to-point</code> 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr></table>		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.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
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.													
8.3.12.0	Introduced on the S4810.													
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.

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
9.7(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.
8.3.11.1	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 [clsns host](#) — defines a name-to-NSAP mapping.

ignore-lsp-errors

Ignore LSPs with bad checksums instead of purging those LSPs.

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
9.7(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.



Version	Description
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.

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
9.7(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.
8.3.11.1	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.

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
9.7(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.
8.3.11.1	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.

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
9.7(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.
8.3.11.1	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.

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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.12.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr></table>		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.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
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.													
8.3.12.0	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.

Syntax	<code>isis hello-interval seconds [level-1 level-2]</code>	
	To return to the default values, use the <code>no isis hello-interval [seconds] [level-1 level-2]</code> 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.12.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> </table>	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.	8.3.12.0	Introduced on the S4810.	8.3.11.1	Introduced on the Z9000.
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.												
8.3.12.0	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.

Syntax	<pre>isis hello-multiplier multiplier [level-1 level-2]</pre> To return to the default values, use the <code>no isis hello-multiplier [multiplier] [level-1 level-2]</code> command.						
Parameters	<table> <tr> <td><i>multiplier</i></td><td>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.</td></tr> <tr> <td><i>level-1</i></td><td>(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This value is the default.</td></tr> <tr> <td><i>level-2</i></td><td>(OPTIONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.</td></tr> </table>	<i>multiplier</i>	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 .	<i>level-1</i>	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This value is the default.	<i>level-2</i>	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 2 adjacencies.
<i>multiplier</i>	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 .						
<i>level-1</i>	(OPTIONAL) Select this value to configure the hello multiplier independently for Level 1 adjacencies. This value is the default.						
<i>level-2</i>	(OPTIONAL) 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> </table>	Version	Description	9.7(0.0)	Introduced on the S6000-ON.		
Version	Description						
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.
8.3.12.0	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.

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
9.7(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.
8.3.11.1	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.

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 <code>level-1</code> 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 <code>level-2</code> 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
9.7(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.
8.3.11.1	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.

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
9.7(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.
8.3.11.1	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.

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
9.7(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.
8.3.11.1	Introduced on the Z9000.

isis password

Configure an authentication password for an interface.

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

<i>encryption-type</i>	(OPTIONAL) Enter 7 to encrypt the password using DES.
<i>hmac-md5</i>	(OPTIONAL) Enter the keywords <code>hmac-md5</code> to encrypt the password using MD5.
<i>password</i>	Assign the interface authentication password.
<i>level-1</i>	(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.
<i>level-2</i>	(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
9.7(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.
8.3.11.1	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.

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 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.
9.0.2.0	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.

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
9.7(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.
8.3.11.1	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.

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
9.7(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.
8.3.11.1	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).

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-1	(OPTIONAL) Enter the keywords <code>level-1</code> to apply the configuration to generation of Level-1 LSPs.
	level-2	(OPTIONAL) Enter the keywords <code>level-2</code> 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
9.7(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.
8.3.11.1	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.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
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.

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
9.7(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.
8.3.11.1	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.

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
9.7(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.
8.3.11.1	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.

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 <code>lsp-refresh-interval</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	
	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.
	9.0.2.0	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 <code>seconds</code> 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

Allows you to configure the maximum number of equal cost paths allowed in a routing table.

 **NOTE:** Enables you to configure a single system wide value that is common for both IPv4 and IPv6 addresses.

Syntax	<code>maximum-paths number</code> To return to the default values, use the <code>no maximum-paths</code> 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 (<i>for IPv4</i>) - CONFIGURATION-ROUTER-ISIS-ADDRESS-FAMILY-IPV6 (<i>for IPv6</i>)

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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

To generate and accept old-style, new-style, or both styles of type, length, and values (TLV), configure a router.

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
9.7(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.
8.3.12.0	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.

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
9.7(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.
8.3.12.0	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.

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
9.7(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.
8.3.11.1	Introduced on the Z9000.

passive-interface

Suppress routing updates on an interface. This command stops the router from sending updates on that interface.

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[/subport] or number 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. The range is from 1 to 128.



- For a VLAN interface, 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
9.7(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.
8.3.11.1	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.

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 <code>connected</code> to redistribute active routes into IS-IS.
rip	Enter the keyword <code>rip</code> to redistribute RIP routes into IS-IS.
static	Enter the keyword <code>static</code> to redistribute user-configured routes into IS-IS.
metric <i>metric-value</i>	(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: • <code>external</code> • <code>internal</code>
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 <i>map-name</i>	(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
9.7(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.
8.3.12.0	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.

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, refer to the relevant *Dell 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.
9.0.2.0	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.



Version	Description
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

```
FTOS(config)#router is
FTOS(config-router_isis)#redistribute bgp 1 level-1 metric 32 metric-type
external route-map rmap-isis-to-bgp
FTOS(config-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.

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

<i>process-id</i>	Enter a number that corresponds to the OSPF process ID to be redistributed. The range is from 1 to 65355.
<i>metric metric-value</i>	(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 .
<i>metric-type</i> {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
9.7(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.
8.3.12.0	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

Allows you to enable the IS-IS routing protocol and to specify an IP IS-IS process.

Syntax `router isis [vrf vrf-name] [tag]`
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
9.7(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

To set the overload bit in zeroth fragment of non-pseudonode LSPs on the router, configure the router. This setting prevents other routers from using it as an intermediate hop in their shortest path first (SPF) calculations.

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
9.7(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.
8.3.11.1	Introduced on the Z9000.
7.8.1.0	Added support for multi-topology ISIS.
6.3.1.0	Introduced.

Usage Information

Set the overload bit when a router experiences problems, such as a memory shortage due to an incomplete link state database which 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 recovered.



NOTE: Enables you to 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.

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
9.7(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.
8.3.7.1	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.

Syntax

```
show isis [vrf vrf-name] database [level-1 | level-2] [local] [detail |
summary] [system-id] [lspid]
```

Parameters

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.

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) Displays the detailed link-state database information of each LSP when specified. If not specified, a summary displays.

summary (OPTIONAL) Displays the summary of link-state database information when specified.

lspid (OPTIONAL) Display only the specified LSP.



system-id (OPTIONAL) Displays the link-state database for system-id.

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
9.7(0.0)	Added supported 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.
8.3.7.1	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.



Field	Description
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
FTOS.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.

Syntax `show isis [vrf vrf-name] graceful-restart detail`

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
9.7(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.

Syntax `show isis [vrf vrf-name] hostname`

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
9.7(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.

Syntax `show isis [vrf vrf-name] interface [interface]`

Parameters

- 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.
- interface*** (OPTIONAL) Enter the following keywords and slot/port[/subport] or number 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 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, refer to the relevant *Dell 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)	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
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.

Syntax `show isis [vrf vrf-name] neighbors [level-1 | level-2] [detail] [interface]`

Parameters

<i>vrf vrf-name</i>	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to display adjacent router information corresponding to that VRF.
<i>level-1</i>	(OPTIONAL) Displays information about Level 1 IS-IS neighbors.
<i>level-2</i>	(OPTIONAL) Displays information about Level 2 IS-IS neighbors.
<i>detail</i>	(OPTIONAL) Displays detailed information about neighbors.
<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a VLAN interface, enter the keyword <code>vlan</code> 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, refer to the relevant *Dell 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)	Added support for VRF. Introduced on the S6000-ON.



Version	Description
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 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.

Syntax `show isis [vrf vrf-name] protocol`

Parameters

vrf <i>vrf-name</i>	(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, refer to the relevant *Dell 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)	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:
    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.

Syntax `show isis [vrf vrf-name] traffic [interface]`

Parameters

<i>vrf vrf-name</i>	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to display IS-IS traffic interface information corresponding to that VRF.
<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port[/subport] as one of the following: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a VLAN interface, enter the keyword <code>vlan</code> 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, refer to the relevant *Dell 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)	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.



Item	Description
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.
Level-1/Level-2 LSPs PSNPs (sent/rcvd)	Displays the number of PSNP LSPs 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.

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 <code>level-2</code> to apply the configuration to Level-2 SPF calculations.
<i>interval seconds</i>	Enter the maximum number of seconds between SPF calculations. The range is from 0 to 120 seconds. The default is 10 seconds .
<i>initial_wait_interval seconds</i>	(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 .
<i>second_wait_interval seconds</i>	(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
9.7(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.
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).



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. The LACP commands in this chapter are supported by Dell Networking OS on the S6000–ON platform.

 **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.

clear lacp counters

Clear port channel counters.

Syntax `clear lacp port-channel-number counters`

Parameters

<i>port-channel-number</i>	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
9.7(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.



Version	Description
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).

Syntax `debug lacp [config | events | pdu [interface-type [in | out]]]`
 To disable LACP debugging, use the `no [config | events | pdu [interface-type [in | out]]]` command.

Parameters	config	(OPTIONAL) Enter the keyword <code>config</code> to debug the LACP configuration.
	events	(OPTIONAL) Enter the keyword <code>events</code> to debug the LACP event information.
	pdu	(OPTIONAL) Enter the keyword <code>pdu</code> to debug the LACP Protocol Data Unit information.
	interface-type in out	(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information:
		- For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. Optionally, enter an <code>in</code> or <code>out</code> parameter: - Receive enter <code>in</code> - Transmit enter <code>out</code>

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
9.7(0.0)	Introduced on the S6000–ON.
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.
8.5.1.0	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.

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
9.7(0.0)	Introduced on the S6000–ON.
8.3.19.0	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 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.

Syntax `lacp port-priority priority-value`

To return to the default setting, use the `no lacp port-priority priority-value` command.

Parameters

<i>priority-value</i>	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
9.7(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.
6.2.1.1	Introduced on the E-Series.

lacp system-priority

Configure the LACP system priority.

Syntax `lacp system-priority priority-value`

Parameters

<i>priority-value</i>	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
9.7(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.
6.2.1.1	Introduced on the E-Series.

port-channel-protocol lacp

Enable LACP on any LAN port.

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
9.7(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.
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.

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 <code>sys-id</code> and the value that identifies a system.
counters	(OPTIONAL) Enter the keyword <code>counters</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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 (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 1/6/1 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
-----
Port      LACP PDU      Marker PDU      Unknown      Illegal
          Xmit Recv    Xmit Recv      Pkts Rx      Pkts Rx
-----
Te 1/6/1  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.



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 \(FEFD\)](#)

The VLAN commands are supported on all the S6000–ON platform.

MAC Addressing Commands

The following commands are related to configuring, managing, and viewing MAC addresses.

mac-address-table aging-time

Specify an aging time for MAC addresses to remove from the MAC address table.

Syntax	<code>mac-address-table aging-time seconds</code>	
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	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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
8.3.1.0	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.
pre-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 static

Associate specific MAC or hardware addresses to an interface and VLANs.

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

<i>mac-address</i>	Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
<i>multicast</i>	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.
<i>output interface</i>	For a unicast MAC address, enter the keyword <code>output</code> then one of the following interfaces for which traffic is forwarded: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128.
<i>output-range interface</i>	For a multicast MAC address, enter the keyword <code>output-range</code> then one of the following interfaces to indicate a range of ports for which traffic is forwarded: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number.
<i>vlan vlan-id</i>	Enter the keyword <code>vlan</code> then a VLAN ID 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.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
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.
pre-6.2.1.1	Introduced on the E-Series.

Example (Unicast) `mac-address-table static 00:01:00:00:00:01 {output Te 1/2/1 vlan 2}`

Example (Multicast) `mac-address-table static 01:00:5E:01:00:01 {multicast vlan 2 output-range Te 1/2/1, Te 1/3/1}`

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.

Syntax `[no] mac-address-table station-move refresh-arp`

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
9.7(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.
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, refer to the “NIC Teaming” section of the Layer 2 chapter in the *Dell Networking OS Configuration Guide*.

mac learning-limit

Limit the maximum number of MAC addresses (static + dynamic) learned on a selected interface.

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	Enter the keyword then the VLAN ID. The range is from 1 to 4094.
	dynamic	(OPTIONAL) Enter the keyword <code>dynamic</code> to allow aging of MACs even though a learning limit is configured.
	station-move-violation	(OPTIONAL) Enter the keywords <code>station-move</code> 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
9.7(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.
8.3.12.0	Deprecated the <code>no-station-move</code> command (replaced by the <code>mac-learning-limit mac-address-sticky</code> command).
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the <code>vlan</code> option on the E-Series.



Version	Description
8.2.1.0	Introduced on the S-Series.
7.7.1.0	Introduced on the C-Series. Added the <code>station-move</code> 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 [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.

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 <code>log</code> to generate a syslog message on a learning-limit violation.
shutdown	Enter the keyword <code>shutdown</code> 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
9.7(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 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.

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
9.7(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.
8.3.12.0	Introduced on the S4810.



Usage Information If you configure `mac-learning-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.

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 <code>log</code> to generate a syslog message on a station move violation.
shutdown-both	Enter the keyword <code>shutdown</code> to shut down both the original and offending interface and generate a syslog message.
shutdown-offending	Enter the keywords <code>shutdown-offending</code> to shut down the offending interface and generate a syslog message.
shutdown-original	Enter the keywords <code>shutdown-original</code> 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
9.7(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 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.

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
9.7(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 S-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Introduced on the E-Series.

show mac-address-table

Display the MAC address table.

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[/subport]]]]]`

Parameters

address <i>mac-address</i>	(OPTIONAL) Enter the keyword <code>address</code> then a MAC address in the <code>nn:nn:nn:nn:nn:nn</code> format to display information on that MAC address.
dynamic	(OPTIONAL) Enter the keyword <code>dynamic</code> to display only those MAC addresses the switch dynamically learns. Optionally, you can also add one of these combinations: <code>address/<i>mac-address</i></code> , <code>interface/<i>interface</i></code> , or <code>vlan <i>vlan-id</i></code> .
static	(OPTIONAL) Enter the keyword <code>static</code> to display only those MAC addresses specifically configured on the switch. Optionally, you can also add one of these combinations: <code>address/<i>mac-address</i></code> , <code>interface/<i>interface</i></code> , or <code>vlan <i>vlan-id</i></code> .



aging-time	Enter the keyword <code>aging-time</code> to display only aging-time information.
interface <i>interface</i>	(OPTIONAL) Enter the keyword <code>interface</code> then the interface type, slot/port[/subport] information: - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
interface <i>interface-type</i>	(OPTIONAL) Instead of entering the keyword <code>interface</code> then the interface type, slot/port[/subport] information, as above, you can enter the interface type, then just a slot number.
vlan <i>vlan-id</i>	(OPTIONAL) Enter the keyword <code>vlan</code> then the VLAN ID to display the MAC address assigned to the VLAN. The range is 1 to 4094.
count	(OPTIONAL) Enter the keyword <code>count</code> , 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
9.7(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.
8.3.12.0	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.
pre-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.



Column Heading Description

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: • gi — Gigabit Ethernet then a slot/port. • po — Port Channel then a number. The range is from 1 to 255 for TeraScale. • te — 10 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: • gi — Gigabit Ethernet followed by a slot/port • po — Port Channel followed by a number. Range for Terascale is from 1 to 255. • te — 10-Gigabit Ethernet followed by a slot/port[/subport].
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.

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
9.7(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.
8.3.1.0	Added the <code>vlan</code> option on the E-Series.
7.7.1.0	Introduced on the C-Series and S-Series.
pre-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.

Syntax `show mac learning-limit [violate-action] [detail] [interface interface]`



Parameters

violate-action	(OPTIONAL) Enter the keywords <code>violate-action</code> to display the MAC learning limit violation status.
detail	(OPTIONAL) Enter the keyword <code>detail</code> to display the MAC learning limit in detail.
interface <i>interface</i>	(OPTIONAL) Enter the keyword <code>interface</code> with the following keywords and slot/port[/subport] or number information: • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> 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
9.7(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.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.3.7.0	Introduced on the S4810.
8.3.1.0	Added the <code>vlan</code> option on the E-Series.
7.7.1.0	Introduced on the C-Series.
7.5.1.0	Added support for the <code>violate-action</code> and <code>detail</code> 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 1/1/1    10        0          0          0
Te 1/2/1     5         0          0          0
Dell#show mac learning-limit interface tengigabithethernet 1/1/1
Interface   Learning  Dynamic   Static     Unknown SA
Slot/port   Limit     MAC count MAC count  Drops
Te 1/1/1    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.

Syntax	<code>default vlan-id <i>vlan-id</i></code> To remove the default VLAN status from a VLAN and VLAN 1 does not exist, use the <code>no default vlan-id <i>vlan-id</i></code> syntax.	
Parameters	<i>vlan-id</i>	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	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.
pre-6.2.1.1	Introduced on the E-Series.

Usage Information	To return VLAN 1 as the Default VLAN, use this command syntax (<code>default-vlan-id 1</code>).
	The Default VLAN contains only untagged interfaces.

Related Commands [interface vlan](#) — configures a VLAN.

description

Add a description about the selected VLAN.

Syntax `description description`

Parameters

description	Enter a text string description to identify the VLAN (80 characters maximum).

Defaults none

Command Modes INTERFACE VLAN

Command History	
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.
7.6.1.0	Introduced on the C-Series and S-Series.
6.3.1.1	Introduced on the E-Series.

Related Commands [show vlan](#) – displays the VLAN configuration.

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.

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
9.7(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.
8.3.1.0	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.

name

Assign a name to the VLAN.

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
9.7(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.
pre-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.

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
9.7(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.
pre-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.

Syntax `show vlan [brief | id vlan-id | name vlan-name]`

Parameters

brief	(OPTIONAL) Enter the keyword <code>brief</code> 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 <i>vlan-id</i>	(OPTIONAL) Enter the keyword <code>id</code> then a number from 1 to 4094. Only information on the VLAN specified is displayed.
name <i>vlan-name</i>	(OPTIONAL) Enter the keyword <code>name</code> then the name configured for the VLAN. Only information on the VLAN named 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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
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.
pre-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 <i>Inactive</i> for inactive VLANs and the word <i>Active</i> 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.

Column Heading Description

- Po = port channel
- Gi = gigabit Ethernet
- Te = ten-gigabit Ethernet

Example

```
Dell#show vlan
```

```
Codes: * - Default VLAN, G - GVRP VLANs, P - Primary, C - Community, I - Isolated
```

```
Q: U - Untagged, T - Tagged, O - Openflow
```

```
    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	Inactive		
	2	Active		U Po1(Te 13/1/1) T Po20(Te 13/6/1), Te 13/25/1 T Te 13/7/1
	3	Active	T Po20(Te 13/6/1)	T Te 13/7/1 U Te 13/1/1
	4	Active	U Po2(Te 13/2/1)	T Po20(Te 13/6/1) T Te 13/7/1
	5	Active	T Po20(Te 13/6/1)	T Te 13/7/1 U Te 13/3/1
	6	Active	U Po3(Te 13/4)	T Po20(Te 13/6/1) T Te 13/7/1
	7	Active	T Po20(Te 13/6/1)	T Te 13/7/1 U Te 13/5/1
P	100	Active	T Po1(Te 1/1/1)	T Te 1/2/1
C	101	Inactive	T Te 1/3/1	
I	102	Inactive	T Te 1/4/1	

```
Dell#
```

Example (VLAN ID)

```
Dell# show vlan id 40
```

```
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
40	Active		M Te 13/47/1

```
Dell#show vlan id 41
```

```
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
41	Active		T Te 13/47/1

```
Dell#show vlan id 42
```

```
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
42   Active                U Te 13/47/1
Dell#
```

Example (Brief)

```
Dell#show vlan br
VLAN  Name  STG  MAC Aging      IP Address
-----
1      0      1800          unassigned
2      0      1800          2.2.2.2/24
3      0      1800          3.3.3.2/24
Dell#
```

Example (Name)

```
Dell(conf)#interface vlan 222
Dell(conf-if-vl-222)#name test
Dell(conf-if-vl-222)#do show vlan name test
```

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
222  Inactive                U Te 1/22/1
Dell(conf-if-vl-222)#
```

Example (OpenFlow instance)

	NUM	Status	Description	Q Ports
*	1	Inactive		
	3	Inactive		
O	6	Inactive		
O	8	Inactive		
O	12	Inactive		O Te 1/10/1

Related Commands

[vlan-stack compatible](#) — enables the Stackable VLAN feature on the selected VLAN.

[interface vlan](#) — configures a VLAN.

tagged

Add a Layer 2 interface to a VLAN as a tagged interface.

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[/subport] 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/subport information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

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, refer to the relevant *Dell 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.
9.0.2.0	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.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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.

Syntax `track ip interface`
To remove the tracking feature from the VLAN, use the `no track ip interface` command.

Parameters

<i>interface</i>	Enter the following keywords and slot/port[/subport] or number information: - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.2(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.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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.

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[/subport] 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/subport information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

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, refer to the relevant *Dell 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.
9.2(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.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-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 of the S6000-ON platform.

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.

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 <code>events</code> to enable debugging of FEFD state changes.
packets	Enter the keyword <code>packets</code> to enable debugging of FEFD to view information on packets sent and received.
<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> 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
9.7(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.
8.3.12.0	Introduced on the S4810.

Legacy E-Series
command.

Related Commands

- [fe fd](#) — enables far-end failure detection on an interface.
- [fe fd reset](#) — enables FEFD globally on the system.

fe fd

Enable Far-End Failure Detection on an interface, set the FEFD interval, or select the FEFD mode.

Syntax

```
fe fd {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 <code>fe fd reset</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> . 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.
	9.0.2.0	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	When you enter <code>no fe fd</code> for an interface and <code>fe fd-global</code> , FEFD is enabled on the interface because the <code>no fe fd</code> command is not retained in the configuration file. To keep the interface FEFD disabled when the global configuration changes, use the <code>fe fd reset</code> command.	
Related Commands	• fe fd disable — disables far-end failure detection on an interface. • fe fd reset — enables FEFD globally on the system. • fe fd mode — changes FEFD mode on an interface.	

fe fd disable

Disable FEFD on an interface only. This command overrides the `fe fd reset` command for the interface.

Syntax	<code>fe fd disable</code>
	To re-enable FEFD on an interface, use the <code>no fe fd disable</code> 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
9.7(0.0)	Introduced on the S6000-ON.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Legacy E-Series command.

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

- [fehd reset](#) — enables FEFD globally on the system.
- [fehd mode](#) — changes FEFD mode on an interface.

fehd interval

Set an interval between control packets.

Syntax `fehd interval seconds`
To return to the default value, use the `no fehd 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 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
9.7(0.0)	Introduced on the S6000-ON.
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

Legacy E-Series
command.

Related Commands

- [fefd](#) — enables far-end failure detection.

fefd mode

Change the FEFD mode on an interface.

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 <code>normal</code> 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 <code>aggressive</code> 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 <code>fefd reset</code> 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
9.7(0.0)	Introduced on the S6000-ON.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
Legacy E-Series command.	

Related Commands

- [fefd](#) — enables far-end failure detection.



fefd reset

Reset all interfaces or a single interface that was in “error-disabled” mode.

Syntax `fefd reset [interface]`

Parameters

interface (OPTIONAL) Enter the following keywords and slot/port[/subport] or number 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.

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
9.7(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.
8.3.12.0	Introduced on the S4810.
Legacy E-Series command.	

Related Commands

- [fefd](#) — enables far-end failure detection.

fefd-global interval

Configure an interval between FEFD control packets.

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
9.7(0.0)	Introduced on the S6000-ON.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.
Legacy E-Series command.	

Related Commands

- [fefd](#) — enables far-end failure detection.
- [fefd-global](#) — enables FEFD globally on the system.

fefd-global

Enable FEFD globally on the system.

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 <code>interval</code> 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 <code>mode normal</code> 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 <code>mode aggressive</code> 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 <code>fefd reset</code> 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
9.7(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.
8.3.12.0	Introduced on the S4810.
Legacy E-Series command.	

Usage Information If you enter only the `fe fd-global` syntax, the mode is normal and the default interval is 15 seconds.

If you disable FEFD globally (`no fe fd-global`), the system does not remove the FEFD interface configuration.

Related Commands

- [fe fd](#) — enables far-end failure detection.
- [fe fd-global interval](#) — configures an interval between FEFD control packets.
- [show fe fd](#) — shows the FEFD command output.

show fe fd

View FEFD status globally or on a specific interface.

Syntax `show fe fd [interface]`

Parameters

interface (OPTIONAL) Enter the following keywords and slot/port[/subport] or number 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.

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
9.7(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
8.3.12.0	Introduced on the S4810.
Legacy E-Series command.	

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 <code>fefd reset</code> 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 <code>fefd reset</code> command.) • unknown (only found when FEFD mode is normal. • locally disabled (interface contains the <code>fefd reset</code> command in its configuration). • Admin Shutdown (interface is disabled with the <code>shutdown</code> command).

Example

```
Dell#show fefd
FEFD is globally 'ON', interval is 10 seconds, mode is 'Aggressive'.
```

INTERFACE	MODE	INTERVAL (second)	STATE
Te 5/1/1	Aggressive	10	Admin Shutdown
Te 5/2/1	Aggressive	10	Admin Shutdown
Te 5/3/1	Aggressive	10	Admin Shutdown
Te 5/4/1	Aggressive	10	Admin Shutdown
Te 5/5/1	Aggressive	10	Admin Shutdown
Te 5/6/1	Aggressive	10	Admin Shutdown
Te 5/7/1	Aggressive	10	Admin Shutdown
Te 5/8/1	Aggressive	10	Admin Shutdown
Te 5/9/1	Aggressive	10	Admin Shutdown
Te 5/10/1	NA	NA	Locally disabled
Te 5/11/1	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.



Link Layer Discovery Protocol (LLDP)

The 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 software implementation of LLDP is based on IEEE standard 801.1ab.

The Dell Networking OS supports the basic LLDP commands on S6000–ON platform.

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).

LLPD Commands

The following are LLDP commands.

advertise dot1-tlv

Advertise dot1 TLVs (Type, Length, Value).

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 <code>port-protocol-vlan-id</code> to advertise the port protocol VLAN identification TLV.
port-vlan-id	Enter the keywords <code>port-vlan-id</code> to advertise the port VLAN identification TLV.
vlan-name	Enter the keywords <code>vlan-name</code> 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- <i>interface</i> -lldp)
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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	Introduced on the S-Series. Added the <code>vlan-name</code> 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.

advertise dot3-tlv

Advertise dot3 TLVs (Type, Length, Value).

Syntax	<code>advertise dot3-tlv {max-frame-size}</code> To remove advertised dot3-tlv, use the <code>no advertise dot3-tlv {max-frame-size}</code> command.

Parameters	max-frame-size Enter the keywords <code>max-frame-size</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.
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 counters

Clear LLDP transmitting and receiving counters for all physical interfaces or a specific physical interface.

Syntax `clear lldp counters interface`

Parameters

interface Enter the following keywords and slot/port[/subport] or number 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.

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
9.7(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.
8.5.1.0	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.

Syntax `clear lldp neighbors {interface}`

Parameters

interface

Enter the following keywords and slot/port[/subport] or number 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.

Defaults none

Command Modes EXEC Privilege

Command History

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.
8.5.1.0	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

Enter the following keywords and slot/port[/subport] or number 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.



all	(OPTIONAL) Enter the keyword <code>all</code> to display information on all interfaces.
events	(OPTIONAL) Enter the keyword <code>events</code> to display major events such as timer events.
packet	(OPTIONAL) Enter the keyword <code>packet</code> to display information regarding packets coming in or going out.
brief	(OPTIONAL) Enter the keyword <code>brief</code> to display brief packet information.
detail	(OPTIONAL) Enter the keyword <code>detail</code> to display detailed packet information.
tx	(OPTIONAL) Enter the keyword <code>tx</code> to display transmit-only packet information.
rx	(OPTIONAL) Enter the keyword <code>rx</code> to display receive-only packet information.
both	(OPTIONAL) Enter the keyword <code>both</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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.
8.3.7.0	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.

disable

Enable or disable LLDP.

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
9.7(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.
7.7.1.0	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.

hello

Configure the rate at which the LLDP control packets are sent to its peer.

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
9.7(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.
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.

mode

To receive or transmit, set LLDP.

Syntax `mode {tx | rx}`
To return to the default, use the `no mode {tx | rx}` command.

Parameters

tx	Enter the keyword <code>tx</code> to set the mode to transmit.
rx	Enter the keyword <code>rx</code> 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
9.7(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.
7.7.1.0	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.

Syntax	<code>multiplier integer</code> To return to the default, use the <code>no multiplier integer</code> command.	
Parameters	<i>integer</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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	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.

Syntax	<code>protocol lldp</code> To disable LLDP globally on the chassis, use the <code>no protocol lldp</code> command.	
Defaults	Enabled.	
Command Modes	CONFIGURATION (conf-lldp)	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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	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.

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
9.7(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.
7.7.1.0	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 [<i>interface</i>] [<i>detail</i>]	
Parameters	<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
	<i>detail</i>	(OPTIONAL) Enter the keyword <code>detail</code> 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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 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.

Usage Information	Omitting the keyword <code>detail</code> displays only the remote chassis ID, Port ID, and Dead Interval.

Example	<pre>R1(conf-if-te-1/31/1)#do show lldp neighbors Loc PortID Rem Host Name Rem Port Id Rem Chassis Id ----- Te 1/21/1 R2 TenGigabitEthernet 2/11/1 00:01:e8:06:95:3e Te 1/31/1 R3 TenGigabitEthernet 3/11/1 00:01:e8:09:c2:4a</pre>



show lldp statistics

Display the LLDP statistical information.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
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#
```

LLDP-MED Commands

The following are the LLDP-MED (Media Endpoint Discovery) commands.

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.

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 <code>priority-tagged</code> 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
9.7(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.
7.7.1.0	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.

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.

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

<i>vlan-id</i>	Enter the VLAN ID. The range is from 1 to 4094.
<i>layer2_priority</i>	Enter the Layer 2 priority. The range is from 0 to 7.
<i>DSCP_value</i>	Enter the DSCP value. The range is from 0 to 63.
<i>priority-tagged number</i>	Enter the keywords <code>priority-tagged</code> 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
9.7(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.
7.7.1.0	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.



advertise med location-identification

To advertise a location identifier, configure the system.

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 <i>value</i>	Enter the keywords <code>coordinate-based</code> then the coordinated based location in hexadecimal value of 16 bytes.
civic-based <i>value</i>	Enter the keywords <code>civic-based</code> then the civic based location in hexadecimal format. The range is from 6 to 255 bytes.
ecs-elin <i>value</i>	Enter the keywords <code>ecs-elin</code> 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
9.7(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.
7.7.1.0	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.



advertise med power-via-mdi

To advertise the Extended Power via MDI TLV, configure the system.

Syntax	<pre>advertise med power-via-mdi</pre> To return to the default, use the <code>no advertise med power-via-mdi</code> command.																
Defaults	unconfigured.																
Command Modes	CONFIGURATION (conf-lldp)																
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr></tbody></table>	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.	7.7.1.0	Introduced on the S-Series.	7.6.1.0	Introduced on the C-Series.
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.																
7.7.1.0	Introduced on the S-Series.																
7.6.1.0	Introduced on the C-Series.																
Usage Information	Advertise the Extended Power via MDI on all ports that are connected to an 802.3af powered, LLDP-MED endpoint device.																
Related Commands	debug lldp interface — debugs LLDP. show lldp neighbors — displays the LLDP neighbors.																

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.

Syntax	<pre>advertise med softphone-voice {vlan-id layer2_priority DSCP_value} {priority-tagged number}</pre> To return to the default, use the <code>no advertise med softphone-voice {vlan-id layer2_priority DSCP_value} {priority-tagged number}</code> command.						
Parameters	<table><tr><td><i>vlan-id</i></td><td>Enter the VLAN ID. The range is from 1 to 4094.</td></tr><tr><td><i>layer2_priority</i></td><td>Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.</td></tr><tr><td><i>DSCP_value</i></td><td>Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.</td></tr></table>	<i>vlan-id</i>	Enter the VLAN ID. The range is from 1 to 4094.	<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.	<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
<i>vlan-id</i>	Enter the VLAN ID. The range is from 1 to 4094.						
<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.						
<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.						



priority-tagged number	Enter the keywords <code>priority-tagged</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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	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.

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.

Syntax	<pre>advertise med streaming-video {vlan-id layer2_priority DSCP_value} {priority-tagged number}</pre> To return to the default, use the <code>no advertise med streaming-video {vlan-id layer2_priority DSCP_value} {priority-tagged number}</code> command.

Parameters	<table><tr><td>vlan-id</td><td>Enter the VLAN ID. The range is from 1 to 4094.</td></tr><tr><td>layer2_priority</td><td>Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.</td></tr><tr><td>DSCP_value</td><td>Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.</td></tr><tr><td>priority-tagged number</td><td>Enter the keywords <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.</td></tr></table>	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 <code>priority-tagged</code> then the Layer 2 priority. The range is from 0 to 7.
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 <code>priority-tagged</code> 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
9.7(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.
7.7.1.0	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.

advertise med video-conferencing

To advertise dedicated video conferencing and other similar appliances that support real-time interactive video, configure the system.

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

<i>vlan-id</i>	Enter the VLAN ID. The range is from 1 to 4094.
<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
<i>priority-tagged number</i>	Enter the keywords <code>priority-tagged</code> 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
9.7(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.
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.

advertise med video-signaling

To advertise video control packets that use a separate network policy than video data, configure the system.

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

<i>vlan-id</i>	Enter the VLAN ID. The range is from 1 to 4094.
<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
<i>priority-tagged</i> <i>number</i>	Enter the keywords <code>priority-tagged</code> 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
9.7(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.
7.7.1.0	Introduced on the S-Series.



Version	Description
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.

advertise med voice

To advertise a dedicated IP telephony handset or other appliances supporting interactive voice services, configure the system.

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

<i>vlan-id</i>	Enter the VLAN ID. The range is from 1 to 4094.
<i>layer2_priority</i>	Enter the Layer 2 priority (C-Series and E-Series only). The range is from 0 to 7.
<i>DSCP_value</i>	Enter the DSCP value (C-Series and E-Series only). The range is from 0 to 63.
<i>priority-tagged number</i>	Enter the keywords <code>priority-tagged</code> 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
9.7(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.
7.7.1.0	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.



advertise med voice-signaling

To advertise when voice control packets use a separate network policy than voice data, configure the system.

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 <code>priority-tagged</code> 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
9.7(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.
7.7.1.0	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.



Microsoft Network Load Balancing

Network Load Balancing (NLB) is a clustering functionality that is implemented by Microsoft on Windows 2000 Server and Windows Server 2003 operating systems. Microsoft NLB clustering allows multiple servers running Microsoft Windows to be represented by one MAC and one IP address to provide transparent failover and load-balancing. The Dell Networking OS does not recognize server clusters by default; you must configure NLB functionality on a switch to support server clusters. The maximum NLB entry limit from 8 to 11 is increased and support for more CAM-ACL to increase.

arp (for Multicast MAC Address)

To associate an IP address with a multicast MAC address in the switch when you configure multicast mode of network load balancing (NLB), use address resolution protocol (ARP).

Syntax	<pre>arp ip-address multicast-mac-address interface</pre> To remove an ARP address, use the <code>no arp ip-address</code> command.						
Parameters	<table> <tr> <td data-bbox="367 913 606 966"><i>ip-address</i></td><td data-bbox="606 913 1466 966">Enter an IP address in dotted decimal format.</td></tr> <tr> <td data-bbox="367 966 606 1050"><i>multicast-mac-address</i></td><td data-bbox="606 966 1466 1050">Enter a 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format for the static MAC address to be used to switch multicast traffic.</td></tr> <tr> <td data-bbox="367 1050 606 1449"><i>interface</i></td><td data-bbox="606 1050 1466 1449"> Enter any of the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - The interface specified here must be one of the interfaces configured using the <code>{output-range output} interface</code> option with the <code>mac-address-table static</code> command. </td></tr> </table>	<i>ip-address</i>	Enter an IP address in dotted decimal format.	<i>multicast-mac-address</i>	Enter a 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format for the static MAC address to be used to switch multicast traffic.	<i>interface</i>	Enter any of the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - The interface specified here must be one of the interfaces configured using the <code>{output-range output} interface</code> option with the <code>mac-address-table static</code> command.
<i>ip-address</i>	Enter an IP address in dotted decimal format.						
<i>multicast-mac-address</i>	Enter a 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format for the static MAC address to be used to switch multicast traffic.						
<i>interface</i>	Enter any of the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - The interface specified here must be one of the interfaces configured using the <code>{output-range output} interface</code> option with the <code>mac-address-table static</code> command.						
Defaults	Not configured.						
Command Modes	CONFIGURATION						
Command History	<table> <tr> <td data-bbox="367 1585 606 1617">Version 9.3(0.0)</td><td data-bbox="606 1585 1466 1690">Added support for association of an IP address with multicast MAC address on the S4810, S4820T, S6000, and Z9000 platforms.</td></tr> </table>	Version 9.3(0.0)	Added support for association of an IP address with multicast MAC address on the S4810, S4820T, S6000, and Z9000 platforms.				
Version 9.3(0.0)	Added support for association of an IP address with multicast MAC address on the S4810, S4820T, S6000, and Z9000 platforms.						
Usage Information	For multicast mode of NLB, to associate an IP address with a multicast MAC address in the switch, use address resolution protocol (ARP) by entering the <code>arp ip-address multicast-mac-address</code> command in Global configuration mode. This setting causes the multicast MAC address to be mapped to the cluster IP address for NLB mode of operation of the switch.						

Related Commands [clear arp-cache](#) — clears dynamic ARP entries from the ARP table.

[show arp](#) — displays the ARP table.

mac-address-table static (for Multicast MAC Address)

For multicast mode of network load balancing (NLB), configure a static multicast MAC address, associate the multicast MAC address with the VLAN used to switch Layer 2 multicast traffic, and add output ports that will receive multicast streams on the VLAN. To delete a configured static multicast MAC address from the MAC address table on the router, enter the `no mac-address-table static multicast-mac-address` command.

Syntax `mac-address-table static multicast-mac-address multicast vlan vlan-id range-output {single-interface | interface-list | interface-range}`

To remove a MAC address, use the `no mac-address-table static multicast-mac-address output interface vlan vlan-id` command.

Parameters

<i>multicast-mac-address</i>	Enter the 48-bit hexadecimal address in nn:nn:nn:nn:nn:nn format.
<i>multicast</i>	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.
<i>output interface</i>	For a multicast MAC address, enter the keyword <code>output</code> then one of the following interfaces for which traffic is forwarded: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
<i>output-range interface</i>	For a multicast MAC address, enter the keyword <code>output-range</code> then one of the following interfaces to indicate a range of ports for which traffic is forwarded: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number.
<i>vlan vlan-id</i>	Enter the keyword <code>vlan</code> then a VLAN ID number from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION

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



Version	Description
9.3(0.0)	Added support for multicast MAC address on the MXL platform.

Example (Multicast) `mac-address-table static 01:00:5E:01:00:01 {multicast vlan 2 output-range Te 1/1/2,Te 1/1/3}`

ip vlan-flooding

Enable unicast data traffic flooding on VLAN member ports.

Syntax `ip vlan-flooding`
To disable, use the `no ip vlan-flooding` command.

Command Modes CONFIGURATION

Command History

Version 9.3(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL platforms

Version	Description
9.3(0.0)	Introduced on the S4810, S4820T, S6000, Z9000, and MXL platforms.

Default Disabled

Usage Information By default this command is disabled. There might be some ARP table entries which are resolved through ARP packets which had Ethernet MAC SA different from MAC information inside the ARP packet. This unicast data traffic flooding occurs only for those packets which use these ARP entries.



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.

The Dell Networking operating system supports MSDP commands on the S6000-ON platform.

clear ip msdp peer

Reset the TCP connection to the peer and clear all the peer statistics.

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
9.7(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.
8.3.7.1	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.

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 <code>rejected-sa</code> 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 <code>local</code> 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
9.7(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.
8.3.7.1	Introduced on the S4810.
7.8.1.0	Added the <code>local</code> option.
7.7.1.0	Added the <code>rejected-sa</code> option.
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.

Syntax `clear ip msdp statistic peer peer-address`

Parameters

peer	Enter the keyword <code>peer</code> to clear the MSDP peer entries.



peer-address Enter the IP address of the MSDP peer.

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
9.7(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.
8.3.7.1	Introduced on the S4810.
7.8.1.0	Added the <code>local</code> option.
7.7.1.0	Added the <code>rejected-sa</code> option.
6.2.1.1	Introduced

ip msdp cache-rejected-sa

Enable an MSDP cache for the rejected source-active entries.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
7.4.1.0	Introduced

Related Commands [show ip msdp sa-cache rejected-sa](#) — displays the rejected SAs in the SA cache.

ip msdp default-peer

Define a default peer from which to accept all source-active (SA) messages.

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

<i>peer address</i>	Enter the peer address in a dotted decimal format (A.B.C.D.)
<i>list name</i>	Enter the keywords <code>list name</code> 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
9.7(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	Added the <code>list</code> option and removed the <code>prefix-list</code> 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.

Syntax	<code>ip msdp log-adjacency-changes</code> To disable logging, use the <code>no ip msdp log-adjacency-changes</code> command.
Defaults	Not configured.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
6.2.1.1	Introduced

ip msdp mesh-group

To be a member of a mesh group, configure a peer.

Syntax	<code>ip msdp mesh-group {name} {peer address}</code> To remove the peer from a mesh group, use the <code>no ip msdp mesh-group {name} {peer address}</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
6.2.1.1	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.

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 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. The range is from 1 to 128.
- For a 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.



Version	Description
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.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
6.2.1.1	Introduced

ip msdp peer

Configure an MSDP peer.

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

<i>peer address</i>	Enter the peer address in a dotted decimal format (A.B.C.D.).
<i>connect-source interface</i>	Enter the keywords <code>connect-source</code> then one of the interfaces and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
<i>description name</i>	(OPTIONAL) Enter the keyword <code>description</code> then a description name (maximum 80 characters) to designate a description for the MSDP peer.
<i>sa-limit number</i>	(OPTIONAL) Enter the maximum number of SA entries in SA-cache. The range is from 1 to 100000. .

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
9.7(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.
8.3.7.0	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 <code>description</code> 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.

Syntax `ip msdp redistribute [list acl-name]`

Parameters

list <i>acl-name</i>	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
9.7(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

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.

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 <code>in</code> to enable incoming SA filtering.
out	Enter the keyword <code>out</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.
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.

Syntax `ip msdp sa-limit number`

To return to the default, use the `no ip msdp sa-limit number` command.

Parameters

<i>number</i>	Enter the maximum number of SA entries in SA-cache. The range is from 1 to 500000.

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
9.7(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.
7.5.1.0	Introduced on the E-Series.

Usage Information Dell Networking OS 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 Dell Networking OS 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.

Syntax	<code>ip msdp shutdown {<i>peer address</i>}</code>	
Parameters	<i>peer address</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.
6.2.1.1	Introduced

ip multicast-msdp

Enable MSDP.

Syntax	<code>ip multicast-msdp</code> To exit MSDP, use the <code>no ip multicast-msdp</code> command.	
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	



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.
9.0.2.0	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.
6.2.1.1	Introduced

show ip msdp

Display the MSDP peer status, SA cache, or peer summary.

Syntax `show ip msdp {peer peer address | sa-cache | summary}`

Parameters

peer <i>peer address</i>	Enter the keyword <code>peer</code> then the peer address in a dotted decimal format (A.B.C.D.).
sa-cache	Enter the keywords <code>sa-cache</code> to display the Source-Active cache.
summary	Enter the keyword <code>summary</code> 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
9.7(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.
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  RPAAddr  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
5.5.5.32       6.6.6.32       Established  Lo 32       20
00:07:17      Peer1
Dell#

```

show ip msdp sa-cache rejected-sa

Display the rejected SAs in the SA cache.

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
9.7(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.
8.3.7.1	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	RPAAddr	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



Multiple Spanning Tree Protocol (MSTP)

Multiple spanning tree protocol (MSTP), as implemented by the Dell Networking operating system, conforms to IEEE 802.1s. This command supports the Dell Networking S6000-ON platform.

debug spanning-tree mstp

Enable debugging of the multiple spanning tree protocol and view information on the protocol.

Syntax	debug spanning-tree mstp [all bpdu interface {in out} events] To disable debugging, enter no debug spanning-tree mstp					
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/subport 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr></table>		Version	Description	9.7(0.0)	Introduced on the S6000-ON.
Version	Description					
9.7(0.0)	Introduced on the S6000-ON.					



Version	Description
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.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.2.1.1	Introduced on the E-Series.

Example

```
Dell#debug spanning-tree mstp bpdu tengigabitethernet 2/1/1 ?
in Receive (in)
out Transmit (out)
```

disable

Globally disable the multiple spanning tree protocol on the switch.

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
9.7(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.
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.

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
9.7(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.
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).

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
9.7(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.
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.

Syntax `max-age seconds`

To return to the default values, use the `no max-age` command.



Parameters	<i>max-age</i> Enter a number of seconds the Dell Networking OS 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.5.1.0</td><td>Introduced.</td></tr> </tbody> </table>	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.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.5.1.0	Introduced.
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.																		
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.																		

msti

Configure multiple spanning tree instance, bridge priority, and one or multiple VLANs mapped to the MST instance.

Syntax	<pre>msti instance {vlan range bridge-priority priority}</pre> To disable mapping or bridge priority, use the <code>no msti instance {vlan range bridge-priority priority}</code> command.
Parameters	<i>msti instance</i> Enter the MSTP instance. The range is from zero (0) to 63. <i>vlan range</i> Enter the keyword <code>vlan</code> then the identifier range value. The range is from 1 to 4094. <i>bridge-priority priority</i> Enter the keywords <code>bridge-priority</code> 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
9.7(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.
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.

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
9.7(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.
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.

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
9.7(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.



Version	Description
pre-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 <code>no disable</code> command while in MULTIPLE SPANNING TREE mode. For more information about the multiple spanning tree protocol, refer to the <i>Dell Networking OS Configuration Guide</i>.
Example	<pre>Dell(conf)#protocol spanning-tree mstp Dell(config-mstp)#no disable</pre>
Related Commands	disable — disables multiple spanning tree.

revision

The revision number for the multiple spanning tree configuration.

Syntax	<pre>revision range</pre> To return to the default values, use the <code>no revision</code> 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 <i>Dell Networking OS Command Line Reference Guide</i>.

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.
9.0.2.0	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.
pre-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.

Syntax	<code>show config</code>
Command Modes	MULTIPLE SPANNING TREE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
6.5.1.0	Introduced on the E-Series.

Example	<pre> 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)# </pre>



show spanning-tree mst configuration

View the multiple spanning tree configuration.

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
9.7(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.
pre-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.

Syntax `show spanning-tree msti [instance-number] [brief]] [guard]`

Parameters

<i>instance-number</i>	(Optional) Enter the multiple spanning tree instance number. The range is from 0 to 63.
brief	(Optional) Enter the keyword <code>brief</code> 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
97(0.0)	Introduced on the S6000-ON.
90.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Support for the optional keyword <code>guard</code> 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 2/1/1) 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 2/6/1) 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 2/7/1) 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 Name	PortID	Prio	Cost	Sts	Cost	Designated Bridge ID	PortID
Te 1/1/1	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 1/1/1	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 occurred 00:00:15 ago on Gi 1/1/1
```

Port 257 (TenGigabitEthernet 1/1/1) 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.
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 1/1/1  5          INCON (Root)   Rootguard
Te 1/2/1  5          FWD            Loopguard
Te 1/3/1  5          EDS (Shut)     Bpduguard
```

spanning-tree

Enable the multiple spanning tree protocol on the interface.

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
97(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.
pre-6.2.1.0	Introduced on the E-Series.



spanning-tree msti

Configure multiple spanning tree instance cost and priority for an interface.

Syntax `spanning-tree msti instance {cost cost | priority priority}`

Parameters

msti instance	Enter the keyword <code>msti</code> and the MST instance number. The range is from zero (0) to 63.
cost cost	(OPTIONAL) Enter the keyword <code>cost</code> then the port cost value. The range is from 1 to 200000. The defaults are: • 100 Mb/s Ethernet interface = 200000 • 1-Gigabit Ethernet interface = 20000 • 10-Gigabit Ethernet interface = 2000 • Port Channel interface with one 100 Mb/s Ethernet = 200000 • Port Channel interface with one 1 Gigabit Ethernet = 20000 • Port Channel interface with one 10 Gigabit Ethernet = 2000 • Port Channel with two 1 Gigabit Ethernet = 18000 • Port Channel with two 10 Gigabit Ethernet = 1800 • Port Channel with two 100 Mbps Ethernet = 180000
priority priority	Enter keyword <code>priority</code> 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
9.7(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.
6.5.1.0	Introduced on the E-Series.



tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

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
9.7(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.
6.5.1.0	Introduced

Usage Information By default, Dell Networking OS 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.



Multicast

The multicast commands are supported by Dell Networking operating system (OS) on all S6000–ON platform.

This chapter contains the following sections:

- [IPv4 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.

Syntax	<code>clear ip mroute [vrf vrf-name] {group-address [source-address] * snooping}</code>	
Parameters	vrf vrf-name (OPTIONAL) Enter the keyword <code>vrf</code> 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 <code>*</code> to clear all multicast routes. snooping Enter the keyword <code>snooping</code> to delete multicast snooping route table entries.	
Command Modes	EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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

Version	Description
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.2.(0.0)	Added support for keyword <code>snooping</code> on the Z9000, S4810, and S4820T.

Version	Description
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.
E-Series legacy command	

Related Commands [show ip pim tib](#) — shows the PIM tree information base.

ip mroute

Assign a static mroute.

Syntax

```
ip mroute [vrf vrf-name] 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

vrf vrf-name (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to assign a static mroute to that VRF.



NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

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, refer to the relevant *Dell 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)	Added support for VRF. 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.
8.3.7.0	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.

Syntax `ip multicast-limit [vrf vrf-name] limit`

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to limit the number of multicast on the VRF.
limit	Enter the desired maximum number of multicast entries on the system. The S-Series range is from 1 to 16000.

Defaults The S-Series default is **4000**.

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)	Added support for VRF. 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.



Version	Description
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.

Syntax `ip multicast-routing [vrf vrf-name]`

To disable multicast forwarding, use the `no ip multicast-routing [vrf vrf-name]` 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
9.7(0.0)	Added support for VRF. 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.
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 mroute

View the multicast routing table.

Syntax `show ip mroute [vrf vrf-name] [static | group-address [source-address] | count | snooping [vlan vlan-idIntroduced on the S6000-ON.] [group-address [source-address]] | 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.

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, refer to the relevant *Dell 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)	Added support for VRF. Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.

Version	Description
9.0.2.0	Introduced on the S6000.
9.2.(0.0)	Added support for keyword <code>vlt</code> to the Z9000, S4810, and S4820T.
8.4.1.1	Support for the keyword <code>snooping</code> and the optional <code>vlan</code> <code>vlan-id</code> , <code>group-address</code> , and <code>source-address</code> 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:
    TenGigabitEthernet 4/13/1

(*, 225.1.2.1), uptime 00:04:16
  Incoming vlan: Vlan 2
  Outgoing interface list:
    TenGigabitEthernet 4/11/1
    TenGigabitEthernet 4/13/1

(165.87.1.7, 225.1.2.1), uptime 00:03:17
  Incoming vlan: Vlan 2
  Outgoing interface list:
    TenGigabitEthernet 4/11/1
    TenGigabitEthernet 4/13/1
    TenGigabitEthernet 4/20/1

```

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

```
Dell#show ip mroute

IP Multicast Routing Table

(*, 224.10.10.1), uptime 00:05:12
  Incoming interface: TenGigabitEthernet 3/12/1
  Outgoing interface list:
    TenGigabitEthernet 3/13/1

(1.13.1.100, 224.10.10.1), uptime 00:04:03
  Incoming interface: TenGigabitEthernet 3/4/1
  Outgoing interface list:
    TenGigabitEthernet 3/12/1
    TenGigabitEthernet 3/13/1

(*, 224.20.20.1), uptime 00:05:12
  Incoming interface: TenGigabitEthernet 3/12/1
  Outgoing interface list:
    TenGigabitEthernet 3/4/1
```

show ip rpf

View reverse path forwarding.

Syntax show ip rpf

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
9.7(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
8.3.7.1	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: Te 3/4/1
  RPF neighbor: 165.87.31.4
  RPF route/mask: 10.10.10.9/255.255.255.255
  RPF type: unicast
```

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

IPv6 Router Advertisement (RA) Guard

The IPv6 RA guard provides support to perform conditional forwarding or blocking of the router advertisement messages that are received at the network device platform. This functionality analyzes and filters the RAs sent by the devices and compares the configuration information on the layer 2 device with the RA frame. Once the layer 2 device validates the content of the RA frame against the configuration, it forwards the RA to its unicast or multicast destination. On failure to validate the RA frame content, the RA frame is dropped.

The IPv6 RA guard supports two different modes:

- Host mode — When a policy with device role as host is applied on an interface, all the RA packets are dropped without validation. You can also configure the host mode policy with VLAN option to drop the RA packets on that specific VLAN and port.
- Router mode — When a policy with device role as router is applied on an interface, all the RA packets are validated based on the configuration information in the policy. Similarly, you can also apply this mode over any specific VLAN and the validation is performed only for that particular VLAN RA packets.

To configure the IPv6 RA guard, use the following Dell Networking OS commands.

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.

Syntax `clear ipv6 neighbors [ipv6-address | interface]`

Parameters

ipv6-address Enter the IPv6 address of the neighbor in the x:x:x:x format to remove a specific IPv6 neighbor.



NOTE: The :: notation specifies successive hexadecimal fields of zero.

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:

- 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.
- 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, refer to the relevant *Dell 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.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.

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/subport 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, 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 <code>host</code> to set the device-role as host.
router	Enter the keyword <code>router</code> 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- [ipv6 nd raguard policy policy-name](#) — Defines the RA guard policy name and enter the RA guard policy configuration mode.
- [ipv6 nd ra-guard enable](#) — Allows you to 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 <i>limit</i>	Enter the keyword <code>maximum</code> then the hop limit value. The range is from 0 to 254.
minimum <i>limit</i>	Enter the keyword <code>minimum</code> 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- [ipv6 nd ra-guard enable](#)—Allows you to configure the RA guard related commands.
- [ipv6 nd ra-guard policy policy-name](#) — Defines 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 <i>policy-name</i>	Enter the keyword <code>policy</code> then the policy name. The policy-name allows a maximum of 140 characters.
vlan [vlan 1, vlan 2, vlan 3.....]	Enter the keyword <code>vlan</code> 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, refer to the relevant *Dell 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.



Version	Description
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands [show ipv6 nd ra-guard policy](#) — Displays 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands [ipv6 nd ra-guard enable](#) — Allows you to configure the RA guard related commands.



ipv6 neighbor

Configure a static entry in the IPv6 neighbor discovery.

Syntax `ipv6 neighbor {ipv6-address} {interface interface} {hardware_address}`
To remove a static IPv6 entry from the IPv6 neighbor discovery, use the `no ipv6 neighbor {ipv6-address} {interface interface}` command.

Parameters

ipv6-address	Enter the IPv6 address of the neighbor in the x:x:x::x format.  NOTE: The :: notation specifies successive hexadecimal fields of zero.
interface interface	Enter the keyword <code>interface</code> then the interface type and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. • For a Null interface, enter the keyword <code>null</code> then the Null interface number. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094. • For a tunnel interface, enter the keyword <code>tunnel</code> then the tunnel interface number. The range is from 1 to 16383.
hardware_address	Enter a 48-bit hardware MAC address in nn:nn:nn:nn:nn:nn format.

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
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.1	Introduced on the S4810.



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 <code>on</code> to set the managed-config-flag value as ON.
off	Enter the keyword <code>off</code> 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- [ipv6 nd ra-guard enable](#) — Allows you to configure the RA guard related commands.
- [ipv6 nd raguard policy policy-name](#) — Defines 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 <code>ipv6-access-list</code> then the access-list name. The access-list name allows a maximum of 140 characters.
ipv6-prefix-list name	Enter the keywords <code>ipv6-prefix-list</code> then the prefix-list name. The prefix-list name allows a maximum of 140 characters.
ipv6-mac-access-list name	Enter the keywords <code>ipv6-mac-access-list</code> 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- [ipv6 nd ra-guard enable](#) — Allows you to configure the RA guard related commands.
- [ipv6 nd raguard policy policy-name](#) — Defines the 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 <i>name</i>	Enter the keywords <code>ipv6-access-list</code> then the access-list name. The access-list name allows a maximum of 140 characters.
ipv6-prefix-list <i>name</i>	Enter the keywords <code>ipv6-prefix-list</code> then the prefix-list name. The prefix-list name allows a maximum of 140 characters.
ipv6-mac-access-list <i>name</i>	Enter the keywords <code>ipv6-mac-access-list</code> 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- [ipv6 nd ra-guard enable](#) — Allows you to configure the RA guard related commands.
- [ipv6 nd raguard policy policy-name](#) — Defines 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands	• ipv6 nd ra-guard enable — Allows you to configure the RA guard related commands. • ipv6 nd raguard policy policy-name — Defines 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	<code>other-config-flag {on off}</code> To reset the other configuration parameter, use the <code>no other-config-flag {on off}</code> command.

Parameters	on Enter the keyword <code>on</code> to set the other-config-flag value as ON.
	off Enter the keyword <code>off</code> 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands	• ipv6 nd ra-guard enable — Allows you to configure the RA guard related commands. • ipv6 nd raguard policy policy-name — Defines 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- [ipv6 nd ra-guard enable](#) — Allows you to configure the RA guard related commands.
- [ipv6 nd raguard policy policy-name](#) — Defines 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-timer value` 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.



Related Commands [ipv6 nd raguard policy policy-name](#) — Defines the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.

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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- [ipv6 nd ra-guard enable](#) — Allows you to configure the RA guard related commands.
- [ipv6 nd raguard policy policy-name](#) — Defines 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, refer to the relevant *Dell 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.



Version	Description
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Related Commands

- [ipv6 nd ra-guard enable](#) — Allow you to configure the RA guard related commands.
- [ipv6 nd ra-guard policy policy-name](#) — Defines 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, 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](#) — Allows you to configure the RA guard related commands.
- [ipv6 nd ra-guard policy](#) — Defines the RA guard policy name and enter the RA guard policy list configuration mode.
- [device-role](#) — Specifies the role of the device attached to the port.
- [hop-limit](#) — Enables the verification of the advertised hop count limit.
- [mtu](#) — Sets the maximum transmission unit (MTU) value.
- [other-config-flag](#) — Enables the verification of the advertised other configuration parameter.
- [reachable-time](#) — Sets the advertised reachability time.
- [retrans-timer](#) — Sets the advertised retransmission time.
- [router-preference maximum](#) — Enables the verification of the advertised default router preference (DRP) value.
- [trusted-port](#) — Applies 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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, 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 1/1/1
Dell#
```

Related Commands

- [ipv6 nd ra-guard enable](#) — Allows you to configure the RA guard related commands.
- [ipv6 nd ra-guard policy](#) — Defines the RA guard policy name and enter the RA guard policy list configuration mode.
- [device-role](#) — Specifies the role of the device attached to the port.
- [hop-limit](#) — Enables the verification of the advertised hop count limit.
- [mtu](#) — Sets the maximum transmission unit (MTU) value.
- [other-config-flag](#) — Enables the verification of the advertised other configuration parameter.
- [reachable-time](#) — Sets the advertised reachability time.
- [retrans-timer](#) — Sets the advertised retransmission time.
- [router-preference maximum](#) — Enables the verification of the advertised default router preference (DRP) value.
- [trusted-port](#) — Applies the policy to trusted ports.
- [ipv6 nd raguard attach-policy](#) — Applies the IPv6 RA guard to a specific interface.



show ipv6 neighbors

Display IPv6 discovery information. Entering the command without options shows all IPv6 neighbor addresses stored on the control processor (CP).

Syntax	<code>show ipv6 neighbors [vrf <i>vrf-name</i>] [<i>ipv6-address</i>] interface <i>interface</i></code>		
Parameters	<i>vrf vrf-name</i>	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to display the neighbors corresponding to the VRF.	 NOTE: If you do not specify this option, neighbors corresponding to the default VRF are displayed.
	<i>ipv6-address</i>	Enter the IPv6 address of the neighbor in the <code>x:x:x:x:x</code> format.	 NOTE: The <code>::</code> notation specifies successive hexadecimal fields of zero.
	<i>interface interface</i>	Enter the keyword <code>interface</code> then the interface type and slot/port or number information: • For a port channel interface, enter the keywords <code>port-channel</code> then a number. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port and number. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port and number. • For a VLAN interface, enter the keyword <code>vlan</code> 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 <i>Dell Networking OS</i> release notes. The following is a list of the Dell Networking OS version history for this command.		

Version	Description
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.

Example

IPv6 Address	Expires (min)	Hardware Address	State
100::1	0.03	00:00:00:00:00:22	DELAY
fe80::200:ff:fe00:22	232	00:00:00:00:00:22	STALE
500::1	0.60	00:01:e8:17:5c:af	REACH
fe80::200:ff:fe00:17	232	00:00:00:00:00:29	REACH
900::1	0.60	00:01:e8:17:5c:b1	STALE
400::1	0.60	00:01:e8:17:5c:ae	REACH

Dell#



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, refer to the relevant *Dell 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.
9.7(0.0)	Introduced on the S4810, S4820T, S5000, S6000, and Z9000 switches.

Usage Information Use this command to disable all the RA guard policies.

Related Commands

- [ipv6 nd ra-guard enable](#) — Allows you to configure the RA guard related commands.
- [ipv6 nd raguard policy policy-name](#) — Defines the router advertisement (RA) guard policy name and enter the RA guard policy configuration mode.



Object Tracking

Object Tracking supports IPv4 and IPv6, and is available on the Dell Networking, C-Series, E-Series, S-Series, and S4810 platforms. 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](#)

IPv4 Object Tracking Commands

The following section describes the IPv4 VRRP commands.

debug track

Enables debugging for tracked objects.

Syntax	debug track [<i>all</i> <i>notifications</i> <i>object-id</i>]	
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 1 to 500.
Defaults	Enable debugging on the state and notifications of all tracked objects (<code>debug track all</code>).	
Command Modes	• EXEC	
	• EXEC Privilege	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	8.3.12.0	Introduced on the S4810.



Version	Description
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.

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

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

You can configure an UP and/or DOWN timer for each tracked object to set the time delay before a change in the state of a tracked object is communicated to clients. 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 no delay is configured, 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.

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

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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.

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
9.7(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.

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
9.7(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 <i>object-id</i>	Displays the number of the tracked object.
Interface <i>type slot/port</i>, IP route <i>ip-address</i>, IPv6 route <i>ipv6-address</i>	Displays the interface type and slot/port number or address of the IPv4/IPv6 route that is being tracked.
<i>object</i> is Up/Down	Up/Down state of tracked object; for example, IPv4 interface, reachability or metric threshold of an IP route.
<i>number</i> changes, last change <i>time</i>	Number of times that the state of the tracked object has changed and the time since the last change in <i>hours:minutes:seconds</i> .
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.

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
```

Usage Information 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 (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.

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 <i>number</i>	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 <i>number</i>	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

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 configure the UP and/or DOWN threshold for the scaled metric of a tracked IPv4 or IPv6 route.

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.

Syntax

```
track object-id interface interface ip routing
```

To return to the default setting, use the `no track object-id` command.

Parameters

<i>object-id</i>	Enter the ID number of the tracked object. The range is 1 to 500.
<i>interface</i>	Enter one of the following values: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Defaults

none

Command Modes

CONFIGURATION

Command History

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 2 interface:

- The status of the IPv4 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 IPv4 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](#) – 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.

Syntax `track object-id interface interface line-protocol`
To return to the default setting, use the `no track object-id` command.

Parameters

<i>object-id</i>	Enter the ID number of the tracked object. The range is 1 to 500.
<i>interface</i>	Enter one of the following values: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Defaults none

Command Modes CONFIGURATION

Command History	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 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.

Syntax `track object-id ip route ip-address/prefix-len metric threshold [vrf vrf-name]`
To return to the default setting, use the `no track object-id` command.

Parameters

<i>object-id</i>	Enter the ID number of the tracked object. The range is 1 to 500.

<i>ip-address/prefix-len</i>	Enter an IPv4 address in dotted decimal format. The valid IPv4 prefix lengths are from /0 to /32.
<i>vrf vrf-name</i>	(Optional) E-Series only: You can configure a VPN routing and forwarding (VRF) instance to specify the virtual routing table to which the tracked route belongs.

Defaults none

Command Modes CONFIGURATION

Command History

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 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.

Syntax `track object-id ip route ip-address/prefix-len reachability [vrf vrf-name]`
To return to the default setting, use the `no track object-id` command.



Parameters	<i>object-id</i>	Enter the ID number of the tracked object. The range is 1 to 500.
	<i>ip-address/ prefix-len</i>	Enter an IPv4 address in dotted decimal format. The valid IPv4 prefix lengths are from /0 to /32.
	<i>vrf vrf-name</i>	(Optional) E-Series only: You can configure a VPN routing and forwarding (VRF) instance to specify the virtual routing table to which the tracked route belongs.

Defaults none

Command Modes CONFIGURATION

Command History

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 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 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](#) – 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 resolution ip route

Configure the protocol-specific resolution value used to scale an IPv4 route metric.

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	<i>object-id</i>	Enter the ID number of the tracked object. The range is 1 to 500.
	<i>isis resolution-value</i>	Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.
	<i>ospf resolution-value</i>	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	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 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 0 to 255. The UP/DOWN state of a tracked IPv4 route is determined by a user-configurable threshold (the <code>threshold metric</code> 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 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 1 to 1000, where the default is 10. • For OSPF, you can set the resolution in the range 1 to 1592, where the default is 1. • The resolution value used to map static routes is not configurable. By default, Dell Networking OS assigns a metric of 0 to static routes. • The resolution value used to map RIP routes is not configurable. 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.

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

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 The following describes the `show track ipv6 route` command shown in the Example below.

Output	Description
Track <i>object-id</i>	Displays the number of the tracked object.
Interface <i>type slot/port</i>, IP route <i>ip-address</i>, IPv6 route <i>ipv6-address</i>	Displays the interface type and slot/port number or address of the IPv4/IPv6 route that is being tracked.
<i>object</i> is Up/Down	Up/Down state of tracked object; for example, IPv4 interface, reachability or metric threshold of an IP route.
<i>number</i> changes, last change <i>time</i>	Number of times that the state of the tracked object has changed and the time since the last change in <i>hours:minutes:seconds</i> .
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.

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 1
```



Usage Command The following describes the show track ipv6 route brief command shown in the Example below.

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 (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.

Syntax `track object-id interface interface ipv6 routing`
To return to the default setting, use the `no track object-id` command.

Parameters

<i>object-id</i>	Enter the ID number of the tracked object. The range is 1 to 500.
<i>interface</i>	Enter one of the following values: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Defaults none

Command Modes CONFIGURATION

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.



Version	Description
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.

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

<i>object-id</i>	Enter the ID number of the tracked object. The range is 1 to 500.
<i>ipv6-address/prefix-len</i>	Enter an IPv6 address in X:X:X:X format. The valid IPv6 prefix lengths are from /0 to / 128.

Defaults none

Command Modes CONFIGURATION

Command History

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 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. 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 IPv6 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 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 1 to 500.
	ipv6-address/ prefix-len	Enter an IPv6 address in X:X:X:X format. The valid IPv6 prefix lengths are from /0 to / 128.

Defaults none

Command Modes CONFIGURATION

Command History	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 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 resolution ipv6 route

Configure the protocol-specific resolution value used to scale an IPv6 route metric.

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

<i>object-id</i>	Enter the ID number of the tracked object. Use the range to 1 to 500.
<i>isis resolution-value</i>	Enter the resolution used to convert the metric in the routing table for ISIS routes to a scaled metric.
<i>ospf resolution-value</i>	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

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 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 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 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 1 to 1000, where the default is 10.
- For OSPF, you can set the resolution in the range 1 to 1592, where the default is 1.
- The resolution value used to map static routes is not configurable. By default, Dell Networking OS assigns a metric of 0 to static routes.
- The resolution value used to map RIP routes is not configurable. 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.



Open Shortest Path First (OSPFv2 and OSPFv3)

Open Shortest Path First version 2 for IPv4 is supported on platform.

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.

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.

• [Open Shortest Path First \(OSPFv2\)](#)

 **NOTE: Dell Networking Operating System (OS) version 7.8.1.0 introduces Multi-Process OSPF on IPv4 (OSPFv2) only. It is not supported on OSPFv3 (IPv6).**

The CLI requires that you include the Process ID when entering ROUTER-OSPF mode. Each command entered applies to the specified OSPFv2 process only.

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.

S6000-ON

Syntax	<code>area area-id default-cost cost</code>	
	To return default values, use the <code>no area area-id default-cost</code> 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	<code>cost = 1</code> ; 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 <i>Dell Networking OS Command Line Reference Guide</i> .	



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.
9.0.2.0	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.

Usage Information In the Dell Networking operating software (OS), `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).

S6000-ON

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 <code>redistribute</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.
7.8.1.0	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.

area range

Summarize routes matching an address/mask at an area border router (ABR).

S6000–ON

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

<i>area-id</i>	Specify the OSPF area in dotted decimal format (A.B.C.D.) or enter a number from zero (0) to 65535.
<i>ip-address</i>	Specify an IP address in dotted decimal format.
<i>mask</i>	Specify a mask for the destination prefix. Enter the full mask (for example, 255.255.255.0).
<i>not-advertise</i>	(OPTIONAL) Enter the keywords <code>not-advertise</code> 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
9.7(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	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.



Version	Description
pre- 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.

S6000-ON

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 <code>no-summary</code> 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
9.7(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	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.

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.

S6000-ON

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 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
9.7(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	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.

clear ip ospf

Clear all OSPF routing tables.

S6000-ON

Syntax `clear ip ospf process-id [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.
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
9.7(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	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.

clear ip ospf statistics

Clear the packet statistics in interfaces and neighbors.

S6000-ON

Syntax

```
clear ip ospf [process-id] [vrf vrf-name] statistics [interface name
{neighbor router-id}]
```

Parameters

<i>process-id</i>	Enter the OSPF Process ID to clear a specific process. If no Process ID is entered, all OSPF processes are cleared.
<i>vrf vrf-name</i>	Enter the keyword <code>vrf</code> followed by the name of the VRF to clear all OSPF routing tables corresponding to that VRF.
<i>statistics</i>	Enter the keyword <code>statistics</code> to clear the packet statistics in interfaces and neighbors.
<i>interface name</i>	(OPTIONAL) Enter the keyword <code>interface</code> then one of the following interface keywords and slot/port or number information: • For Port Channel groups, enter the keywords <code>port-channel</code> then a number. For the C-Series and S-Series, the range is from 1 to 128. • For a SONET interface, enter the keyword <code>sonet</code> then the slot/ port information. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
<i>neighbor router-id</i>	(OPTIONAL) Enter the keyword <code>neighbor</code> 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

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.

S6000-ON

Syntax `debug ip ospf [process-id] [vrf vrf-name] [bfd | event | packet | spf | database-timer rate-limit]`

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.
	bfd	(OPTIONAL) Enter the keyword <code>bfd</code> to debug only OSPF BFD information.
	event	(OPTIONAL) Enter the keyword <code>event</code> to debug only OSPF event information.
	packet	(OPTIONAL) Enter the keyword <code>packet</code> to debug only OSPF packet information.
	spf	(OPTIONAL) Enter the keyword <code>spf</code> to display the Shortest Path First information.
	database-timer rate-limit	(OPTIONAL) Enter the keywords <code>database-timer rate-limit</code> to display the LSA throttling timer information. This applies to the S4810 platform only.

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
9.0.2.0	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 <code>database-timer rate-limit</code> 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.
pre- 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. Dell Networking OS 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 <code>ip ospf authentication-key</code> command • 2 - MD5 authentication configured using the <code>ip ospf message-digest-key</code> command
auk:	If the <code>ip ospf authentication-key</code> command is configured, this field displays the key used.
keyid:	If the <code>ip ospf message-digest-key</code> command is configured, this field displays the MD5 key
to:	Displays the interface to which the packet is intended.



Field	Description
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.
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) 1:44 rid:192.1.1.1
aid:0.0.0.1 chk:0xa098 aut:0 auk: keyid:0 to:Te 4/3/1 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 Dell Networking Operating System (OS).

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 <code>always</code> to specify that default route information must always be advertised.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number to configure a metric value for the route. The range is from 1 to 16777214.
metric-type <i>type-value</i>	(OPTIONAL) Enter the keywords <code>metric-type</code> 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
9.7(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	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.

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.

S6000-ON

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
9.7(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.
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.

description

Add a description about the selected OSPF configuration.

S6000-ON

Syntax	<code>description description</code> To remove the OSPF description, use the <code>no description</code> 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

Related Commands [show ip ospf asbr](#) — displays the VLAN configuration.



distance

Define an administrative distance for particular routes to a specific IP address.

S6000-ON

Syntax	<code>distance weight [ip-address mask access-list-name]</code> To delete the settings, use the <code>no distance weight [ip-address mask access-list-name]</code> 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.
	access-list-name	(OPTIONAL) Enter the name of an IP standard access 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

distance ospf

Configure an OSPF distance metric for different types of routes.

S6000-ON

Syntax	<code>distance ospf [external dist3] [inter-area dist2] [intra-area dist1]</code> To delete these settings, use the <code>no distance ospf</code> command.



Parameters	external <i>dist3</i>	(OPTIONAL) Enter the keyword <code>external</code> 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 <i>dist2</i>	(OPTIONAL) Enter the keywords <code>inter-area</code> 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 <i>dist1</i>	(OPTIONAL) Enter the keywords <code>intra-area</code> 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 <i>dist3</i> = 110
	· inter-area <i>dist2</i> = 110
	· intra-area <i>dist1</i> = 110

Command Modes	ROUTER OSPF

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

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.
9.0.2.0	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.
6.1.1.1	Introduced on the E-Series.

Usage Information	To specify a distance for routes learned from other routing domains, use the <code>redistribute</code> command.

distribute-list in

Apply a filter to incoming routing updates from OSPF to the routing table.

S6000-ON

Syntax	<code>distribute-list <i>prefix-list-name</i> in [<i>interface</i>]</code>
	To delete a filter, use the <code>no distribute-list <i>prefix-list-name</i> in [<i>interface</i>]</code> command.

Parameters	<i>prefix-list-name</i>	Enter the name of a configured prefix list.
	<i>interface</i>	(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. For the C-Series, S-Series, and Z9000, the range is from 1 to 128. For Z9500, the range is from 1 to 512.
- For a SONET interface, enter the keyword `sonet` 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 VLAN, enter the keyword `vlan` then a number from 1 to 4094.

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
9.7(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 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.

distribute-list out

To restrict certain routes destined for the local routing table after the SPF calculation, apply a filter.

S6000-ON

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 <code>connected</code> to specify that connected routes are distributed.
isis	(OPTIONAL) Enter the keyword <code>isis</code> 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 <code>rip</code> 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 <code>static</code> 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
9.7(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	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.

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.

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.

S6000-ON

Syntax `fast-convergence {number}`
To cancel fast-convergence, use the `no fast convergence` command.

Parameters	<i>number</i> 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.8.1.0</td><td>Introduced on all platforms.</td></tr> </tbody> </table>	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.	7.8.1.0	Introduced on all platforms.
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.														
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.														

flood-2328

Enable RFC-2328 flooding behavior.

S6000-ON

Syntax	<code>flood-2328</code> To disable, use the <code>no flood-2328</code> command.								
Defaults	Disabled.								
Command Modes	ROUTER OSPF								
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> </tbody> </table>	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.
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.								



Version	Description
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

In OSPF, flooding is the most resource-consuming task. The flooding algorithm, described in RFC-2328, requires that OSPF flood LSAs (Link State Advertisements) on all interfaces, as governed by LSA's flooding scope (see Section 13 of the RFC). When multiple direct links connect two routers, the RFC-2328 flooding algorithm generates significant redundant information across all links.

By default, Dell Networking OS implements an enhanced flooding procedure that dynamically and intelligently determines when to optimize flooding. Whenever possible, the OSPF task attempts to reduce flooding overhead by selectively flooding on a subset of the interfaces between two routers.

When you enable `flood-2328` , this command configures Dell Networking OS to flood LSAs on all interfaces.

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.

 **NOTE:** This command enables OSPFv2 graceful restart globally by setting the grace period (in seconds) that an OSPFv2 router's neighbors continues to advertise the router as adjacent during a graceful restart.

S6000-ON

Syntax `graceful-restart grace-period seconds`
To disable the grace period, use the `no graceful-restart grace-period` command.

Parameters

<i>seconds</i>	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
9.7(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.
7.8.1.0	Introduced on the S-Series. Added support for Multi-Process OSPF.
7.5.1.0	Introduced on the C-Series.
pre- 6.1.1.1	Introduced on the E-Series.

Usage Information The Helper mode is enabled by default on the device. To enable the restart mode also on the device, you must configure the grace period using this command. After you enable restart mode the router advertises the neighbor as fully adjacent during a restart.

graceful-restart helper-reject

Specify the OSPF router to not act as a helper during graceful restart.

S6000-ON

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
9.7(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.
8.3.12.0	Introduced on the S4810.
7.8.1.0	<code>Restart role</code> enabled on the S-Series (Both <code>Helper</code> and <code>Restart</code> roles now supported on S-Series). Added support for Multi-Process OSPF.
7.7.1.0	Added <code>Helper-Role</code> support on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre- 6.1.1.1	Introduced on the E-Series.



graceful-restart mode

Enable the graceful restart mode.

S6000-ON

Syntax	<code>graceful-restart mode [planned-only unplanned-only]</code> To disable graceful restart mode, use the <code>no graceful-restart mode</code> command.	
Parameters	planned-only	(OPTIONAL) Enter the keywords <code>planned-only</code> to indicate graceful restart is supported in a planned restart condition only.
	unplanned-only	(OPTIONAL) Enter the keywords <code>unplanned-only</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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 on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre- 6.1.1.1	Introduced on the E-Series.

graceful-restart role

Specify the role for your OSPF router during graceful restart.

S6000-ON

Syntax	<code>graceful-restart role [helper-only restart-only]</code> To disable graceful restart role, use the <code>no graceful-restart role</code> command.	
Parameters	role helper-only	(OPTIONAL) Enter the keywords <code>helper-only</code> to specify the OSPF router is a helper only during graceful restart.
	role restart-only	(OPTIONAL) Enter the keywords <code>restart-only</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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-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.
pre- 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.

S6000-ON

Syntax	<code>ip ospf auth-change-wait-time seconds</code> To return to the default, use the <code>no ip ospf auth-change-wait-time</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre- 6.1.1.1	Introduced on the E-Series.

ip ospf authentication-key

Enable authentication and set an authentication key on OSPF traffic on an interface.

S6000-ON

Syntax	<code>ip ospf authentication-key [<i>encryption-type</i>] <i>key</i></code> To delete an authentication key, use the <code>no ip ospf authentication-key</code> command.	
Parameters	<i>encryption-type</i>	(OPTIONAL) Enter 7 to encrypt the key.
	<i>key</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.
pre- 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.

S6000-ON

Syntax	<pre>ip ospf cost cost</pre>



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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
pre- 6.1.1.1	Introduced on the E-Series.

Usage Information	If this command is not configured, cost is based on the <code>auto-cost</code> command. When you configure OSPF over multiple vendors, to ensure that all routers use the same cost, use the <code>ip ospf cost</code> 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.

S6000-ON

Syntax	<code>ip ospf dead-interval seconds</code> To return to the default values, use the <code>no ip ospf dead-interval</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .



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.
9.0.2.0	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.
pre- 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.

S6000-ON

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
9.7(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.
pre- 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.

S6000-ON

Syntax `ip ospf message-digest-key keyid md5 key`
To delete a key, use the `no ip ospf message-digest-key keyid` command.

Parameters

<i>keyid</i>	Enter a number as the key ID. The range is from 1 to 255.
<i>key</i>	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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
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.
pre- 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. Dell Networking OS 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.

S6000-ON

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
9.7(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.
pre- 6.1.1.1	Introduced on the E-Series.

ip ospf network

Set the network type for the interface.

S6000-ON

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 <code>broadcast</code> to designate the interface as part of a broadcast network.
point-to-point	Enter the keywords <code>point-to-point</code> to designate the interface as part of a point-to-point network.

Defaults Broadcast.

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
9.7(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	Added support for 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.

ip ospf priority

To determine the designated router for the OSPF network, set the priority of the interface.

S6000-ON

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
9.7(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.



Version	Description
pre- 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.

S6000-ON

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
9.7(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.
pre- 6.1.1.1	Introduced on the E-Series.

Usage Information Set the time interval to a number large enough to prevent unnecessary retransmissions.



ip ospf transmit-delay

To send a link state update packet on the interface, set the estimated time elapsed.

S6000-ON

Syntax	<code>ip ospf transmit-delay seconds</code> To return to the default value, use the <code>no ip ospf transmit-delay</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> . 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.
9.0.2.0	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.
pre- 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 Dell Networking OS.

S6000-ON

Syntax	<code>log-adjacency-changes</code> To disable the Syslog messages, use the <code>no log-adjacency-changes</code> command.	
Defaults	Disabled.	
Command Modes	ROUTER OSPF	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	



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.
9.0.2.0	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.
pre- 6.1.1.1	Introduced on the E-Series.

maximum-paths

Enable the software to forward packets over multiple paths.

S6000-ON

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, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
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.



Version	Description
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.

mib-binding

Enable this OSPF process ID to manage the SNMP traps and process SNMP queries.

S6000-ON

Syntax	<pre>mib-binding</pre> To mib-binding on this OSPF process, use the <code>no mib-binding</code> command.
Defaults	none.
Command Modes	ROUTER OSPF
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 to all platforms.

Usage Information	This command is either enabled or disabled. If no OSPF process is identified as the MIB manager, the first OSPF process is used. If an OSPF process has been selected, it must be disabled prior to assigning new process ID the MIB responsibility.

network area

Define which interfaces run OSPF and the OSPF area for those interfaces.

S6000-ON

Syntax	<pre>network ip-address mask area area-id</pre> To disable an OSPF area, use the <code>no network ip-address mask area area-id</code> 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
9.7(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 to all platforms.
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.

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.

S6000-ON

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 <code>default</code> to make all OSPF interfaces (current and future) passive.

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 Port Channel groups, enter the keywords `port-channel` then a number. For the C-Series, S-Series, and Z9000, the range is from 1 to 128.
- 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 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
9.7(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	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 <code>default</code> .
pre- 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.

On configuring suppression using the `passive-interface` command, the state of the OSPF neighbor does not change to INIT; instead, the state of the OSPF neighbor changes to DOWN after the dead-timer expires.

redistribute

Redistribute information from another routing protocol throughout the OSPF process.

S6000-ON

Syntax

```
redistribute {connected | isis | ospf | 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 <code>connected</code> to specify that information from active routes on interfaces is redistributed.
isis	Enter the keyword <code>isis</code> to specify that ISO IS-IS information is redistributed.
ospf	Enter the keyword <code>ospf</code> to specify that information corresponding to OSPF is redistributes.
rip	Enter the keyword <code>rip</code> to specify that RIP routing information is redistributed.
static	Enter the keyword <code>static</code> to specify that information from static routes is redistributed.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number. The range is from 0 (zero) to 16777214.
metric-type <i>type-value</i>	(OPTIONAL) Enter the keywords <code>metric-type</code> then one of the following: • 1 = OSPF External type 1 • 2 = OSPF External type 2

route-map <i>map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of the route map.
tag <i>tag-value</i>	(OPTIONAL) Enter the keyword <code>tag</code> 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
9.7(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	Added support for 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.

Usage Information To redistribute the default route (0.0.0.0/0), configure the `default-information originate` command.
Despite removing an OSPF process globally, the OSPF process is not completely removed from the BGP configuration.

Related Commands [default-information originate](#) — generates a default route into the OSPF routing domain.

redistribute bgp

Redistribute BGP routing information throughout the OSPF instance.

S6000-ON

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 <i>number</i>	Enter the autonomous system number. The range is from 1 to 65535.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then the metric-value number. The range is from 0 to 16777214.



metric-type type-value	(OPTIONAL) Enter the keywords <code>metric-type</code> 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 <code>route-map</code> then the name of the route map.
tag tag-value	(OPTIONAL) Enter the keyword <code>tag</code> 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
9.7(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.
7.8.1.3	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 <code>default</code> .
pre- 6.1.1.1	Introduced on the E-Series.

redistribute isis

Redistribute IS-IS routing information throughout the OSPF instance.

S6000-ON

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 <code>level-1</code> to redistribute only IS-IS Level-1 routes.



level-1-2	(OPTIONAL) Enter the keywords <code>level-1-2</code> to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keywords <code>level-2</code> to redistribute only IS-IS Level-2 routes.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number. The range is from 0 (zero) to 4294967295.
metric-type <i>type-value</i>	(OPTIONAL) Enter the keywords <code>metric-type</code> then one of the following: • 1 = for OSPF External type 1 • 2 = for OSPF External type 2
route-map <i>map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> then the name of the route map.
tag <i>tag-value</i>	(OPTIONAL) Enter the keyword <code>tag</code> 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
9.7(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	Added support for Multi-Process OSPF.
7.5.1.0	Introduced on the C-Series.
pre- 6.1.1.1	Introduced on the E-Series.

router-id

To configure a fixed router ID, use this command.

S6000-ON

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
9.7(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	Added support for 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.

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.

S6000-ON

Syntax `router ospf process-id`
To clear 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.

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.
9.0.2.0	Introduced on the S6000.
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.
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.
pre- 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.

Example

```
Dell(config)#router ospf 2
Dell(config-router_ospf)#
```

show config

Display the non-default values in the current OSPF configuration.

S6000-ON

Syntax `show config`

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
9.7(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.
pre- 6.1.1.1	Introduced on the E-Series.



Example

```
Dell(conf-router_ospf)#show config
!
router ospf 3
passive-interface 0 TenGigabitEthernet 1/1/1
Dell(conf-router_ospf)#
```

show ip ospf

Display information on the OSPF process configured on the switch.

S6000-ON

Syntax `show ip ospf [process-id]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

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
9.7(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	Added output for LSA throttling timers.
8.3.7.0	Introduced on the S4810.
7.9.1.0	Added support for VRF.
7.8.1.0	Added support of Multi-Process OSPF.
7.8.1.0	Added the <i>process-id</i> 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.
pre- 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.



Line Beginning with	Description
"Supports only..."	Displays the number of Type of Service (TOS) routes 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-vrf
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.

S6000-ON

Syntax	<code>show ip ospf [process-id vrf vrf-name] asbr</code>	
Parameters	<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
Defaults	none	
Command Modes	- EXEC - EXEC Privilege	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.



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 of Multi-Process OSPF.
7.8.1.0	Added the <i>process-id</i> 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 lasbr

RouterID  Flags    Cost Nexthop  Interface Area
3.3.3.3   -/-/-/   2    10.0.0.2   Te 1/1/1    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.

S6000-ON

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.
- 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
9.7(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	Added support of 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.

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.

S6000-ON

Syntax `show ip ospf [process-id | vrf vrf-name] database asbr-summary [link-state-id] [adv-router ip-address]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(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
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> 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
9.7(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	Added support for 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.

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.

Syntax `show ip ospf [process-id] database external [link-state-id] [adv-router ip-address]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(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
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> 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
9.7(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	Added support for 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.

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:

Field	Description
	• 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.

Syntax	<code>show ip ospf [<i>process-id</i>] database network [<i>link-state-id</i>] [<i>adv-router ip-address</i>]</code>	
Parameters	<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
	<i>link-state-id</i>	(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
	<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.
pre-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.
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.

Syntax `show ip ospf [process-id] database nssa-external [link-state-id] [adv-router ip-address]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(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
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> and the <code>ip-address</code> 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
9.7(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	Added support for 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.

Related Commands [show ip ospf database](#) — displays OSPF database information.



show ip ospf database opaque-area

Display the opaque-area (type 10) LSA information.

Syntax `show ip ospf [process-id] database opaque-area [link-state-id] [adv-router ip-address]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(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
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> 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
9.7(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	Added support for 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.

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:



Item	Description
	• 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.
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.

Syntax	<code>show ip ospf <i>process-id</i> database opaque-as [<i>link-state-id</i>] [<i>adv-router ip-address</i>]</code>	
Parameters	<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.



<i>link-state-id</i>	(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
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> 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
9.7(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	Added support for 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.

Related Commands [show ip ospf database](#) — displays OSPF database information.

show ip ospf database opaque-link

Display the opaque-link (type 9) LSA information.

Syntax	<code>show ip ospf [<i>process-id</i>] database opaque-link [<i>link-state-id</i>] [<i>adv-router ip-address</i>]</code>	
Parameters	<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
	<i>link-state-id</i>	(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, refer to the relevant *Dell 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.
9.0.2.0	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.
pre-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.

Syntax

```
show ip ospf [process-id] 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.

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, refer to the relevant *Dell 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.
9.0.20	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.
pre-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.
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.



Item	Description
(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.

Syntax `show ip ospf [process-id] database summary [link-state-id] [adv-router ip-address]`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>link-state-id</i>	(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
<i>adv-router ip-address</i>	(OPTIONAL) Enter the keywords <code>adv-router</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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.
pre-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:



Item	Description
	• 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

```



Dell#

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.

Syntax	<code>show ip ospf [process-id vrf vrf-name] interface [interface]</code>	
Parameters	<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
	<i>vrf vrf-name</i>	Enter the keyword <code>vrf</code> followed by the name of the VRF to show the OSPF processes that are tied to a specific VRF.
	<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a Null interface, enter the keyword <code>null</code> then the Null interface number. • For a VLAN interface, enter the keyword <code>vlan</code> 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, refer to the relevant *Dell 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.
9.4.(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.
7.8.1.0	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.
pre-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
GigabitEthernet...	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 1/7/1 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 1/8/1 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.

Syntax `show ip ospf [process-id] neighbor`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first 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
9.7(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	Added support for 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.

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 FTOS 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 1/1/1 0.0.0.2
```



```

192.10.10.2 1 FULL/DR      00:00:37 192.10.10.2 Te 1/2/1 0.0.0.1
20.20.20.1  1 FULL/DROTHER 00:00:36 192.10.10.4 Te 1/3/1 0.0.0.1
Dell#

```

show ip ospf routes

Display routes OSPF calculates and stores in OSPF RIB.

Syntax `show ip ospf [process-id] 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.

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
9.7(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	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.





NOTE: Starting with Version 9.4(0.0), the loopback IP address advertised to the neighbor is not displayed in the output because they are not accounted as inactive OSPF routes, whereas the loopback IP address is displayed until Dell Networking OS Version 9.3(0.0). Starting with Version 9.4(0.0), the show ip ospf routes command displays the interface and area ID information of connected networks in addition to the other settings, whereas these details are not displayed until Dell Networking OS Version 9.3(0.0). Starting with Version 9.4(0.0), the metric of E2 routes in the output is displayed as an external metric, whereas until Dell Networking OS Version 9.3(0.0), the number of hops to the ASBR for E2 routes are displayed in the output.

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 1/4/1	1	Intra-Area
13.0.0.0	1	0.0.0.0	Te 1/4/1	0	Intra-Area
150.150.150.0	2	13.0.0.3	Te 1/4/1	-	External
172.30.1.0	2	13.0.0.3	Te 1/4/1	1	Intra-Area

```
Dell#
```

show ip ospf statistics

Display OSPF statistics.

Syntax

```
show ip ospf [process-id | vrf vrf-name] statistics global | [interface  
name {neighbor router-id}]
```

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.
<i>vrf vrf-name</i>	Enter the keyword <code>vrf</code> followed by the name of the VRF to display statistics corresponding to the OSPF process that is tied to a specific VRF.
<i>global</i>	Enter the keyword <code>global</code> to display the packet counts received on all running OSPF interfaces and packet counts OSPF neighbors receive and transmit.
<i>interface name</i>	(OPTIONAL) Enter the keyword <code>interface</code> then one of the following interface keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
<i>neighbor router-id</i>	(OPTIONAL) Enter the keyword <code>neighbor</code> 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, refer to the relevant *Dell 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.
9.4.(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.
7.8.1.0	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.

Example

```

Dell#show ip ospf 1 statistics global

OSPF Packet Count
  Total Error Hello DDiscr LSReq LSUpd LSAck
RX 10    0    8    2    0    0    0
TX 10    0   10    0    0    0    0

OSPF Global Queue Length
  TxQ-Len RxQ-Len Tx-Mark Rx-Mark
Hello-Q   0     0     0     2
LSR-Q     0     0     0     0
Other-Q   0     0     0     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-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   Unkown-Pkt 0

Error packets (Only for TX)

Socket Errors    0
Dell#

```

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(conf-if-te-1/6/1)#do show ip ospf statistics
Interface TenGigabitEthernet 1/6/1
  Error packets (Receive statistics)
    Intf-Down 0 Non-Dr 0 Self-Orig 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-IsReq 0
    RtidZero 0
  Neighbor ID 4.4.4.4
    Packet Statistics
      Hello DDiscr LSReq LSUpd LSAck
      RX 5 2 1 3 2
      TX 6 5 1 3 3
    Timers
      Hello 0 Wait 0 Grace 0
      Dead 39 Transmit 4
    Queue Statistics
      LSU-Q-Len 0 LSU-Q-Wmark 1
      LSR-Q-Len 0 LSR-Q-Wmark 1

Dell(conf-if-te-1/6/1)#
```

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.

Syntax `show ip ospf [process-id] 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.

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
97(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	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.

Syntax `show ip ospf [process-id] topology`

Parameters

<i>process-id</i>	Enter the OSPF Process ID to show a specific process. If no Process ID is entered, command applies only to the first OSPF process.

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
97(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	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 Gi 13/1   0
1.1.1.1    E/-/-/ 1    10.0.0.1 Gi 7/1    1
Dell#
```

summary-address

To advertise one external route, set the OSPF ASBR.

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

<i>ip-address</i>	Specify the IP address in dotted decimal format of the address to summarize.
<i>mask</i>	Specify the mask in dotted decimal format of the address to summarize.
<i>not-advertise</i>	(OPTIONAL) Enter the keywords <code>not-advertise</code> to suppress that match the network prefix/mask pair.
<i>tag tag-value</i>	(OPTIONAL) Enter the keyword <code>tag</code> 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
9.7(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	Added support for 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.

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.

S6000-ON

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, refer to the relevant *Dell 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.
9.2(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.
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#  
Dell#conf
```



```

Dell(conf)#router ospf 1
Dell(conf-router_ospf-1)#timer spf 2 5
Dell(conf-router_ospf-1)#
Dell(conf-router_ospf-1)#show config
!
router ospf 1
timers spf 2 5
Dell(conf-router_ospf-1)#
Dell(conf-router_ospf-1)#end
Dell#
Dell#

```

timers throttle lsa all

Configure LSA transmit intervals.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
9.0.2.0	Introduced on the S6000..
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, then 4000 until 100,000 msec is reached.

timers throttle lsa arrival

Configure the LSA acceptance intervals.

Syntax	<pre>timers throttle lsa arrival arrival-time</pre> To return to the default, use the <code>no timers throttle lsa</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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

Version	Description
97(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	Introduced on the S4810.

OSPFv3 Commands

Open shortest path first version 3 (OSPFv3) for IPv6 is supported on the platform.

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 OSPFv3 area.

Syntax	<pre>area area-id authentication ipsec spi number {MD5 SHA1} [key-encryption-type] key</pre>



Parameters

area <i>area-id</i>	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 <i>number</i>	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
91.(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.

Syntax `area area-id encryption ipsec spi number esp encryption-algorithm [key-encryption-type] key authentication-algorithm [key-encryption-type] key`

Parameters	area <i>area-id</i>	Area for which OSPFv3 traffic is to be encrypted. For <i>area-id</i> , enter a number. The range is from 0 to 4294967295.
	ipsec spi <i>number</i>	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
9.1.(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.

clear ipv6 ospf process

Reset an OSPFv3 router process without removing or re-configuring the process.

Syntax `clear ipv6 ospf [vrf vrf-name] process`



Parameters

vrf <i>vrf-name</i>	(Optional) Enter the keyword vrf followed by 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, refer to the relevant *Dell 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)	Added support for VRF.
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 the E-Series.

debug ipv6 ospf bfd

Display debug information and interface types for bidirectional forwarding detection (BFD) on OSPF IPv6 packets.

Syntax

```
[no] debug ipv6 ospf bfd [interface]
```

Parameters

<i>interface</i>	(OPTIONAL) Enter one of the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/support information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a VLAN interface, enter the keyword <code>vlan</code> 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
9.2(1.0)	Introduced on the Z9500.



Version	Description
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-1/2/1)#do debug ipv6 ospf bfd te 1/2/1
OSPFv3 bfd related debugging is on for TenGigabitEthernet 1/2/1
00:59:26 : OSPFv3INFO: Received Interface mode bfd config command on
interface Te 1/2/1 Enable 1, interval 0, min_rx 0, Multiplier 0, role 0,
Disable 0
00:59:26 : OSPFv3INFO: Enabling BFD on interface Te 1/2/1 Cmd Add Session
00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP
fe80:0000:0000:0201:e8ff:fe8b:7720
00:59:27 : OSPFv3INFO: Completed Enabling BFD on interface Te 1/2/1
00:59:27 : OSPFv3INFO: Completed Interface mode BFD configuration on Te
1/2/1!!
00:59:27 : OSPFv3INFO: Enabling BFD for NBRIP
fe80:0000:0000:0201:e8ff:fe8b:7720
00:59:27 : OSPFv3INFO: Ospf3_register_bfd ospf key 27648
00:59:27 : OSPFv3INFO: OSPFV3 Enabling BFD for NBRIP
fe80:0000:0000:0201:e8ff:fe8b:7720 Interface Te 1/2/1 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
fe80:0000:0000:0201: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 1/2/1 (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
1/2/1 (diag: NO_DIAG)
00:59:45 : OSPFv3INFO: OSPFV3 got BFD msg
00:59:45 : OSPFv3INFO: Bfd Msg Type Up for interface Te 1/2/1
00:59:45 : OSPFv3INFO: OSPFV3 updating NBR state
```

debug ipv6 ospf packet

Display debug information and interface types on OSPF IPv6 packets.

Syntax debug ipv6 ospf {packet | events} [*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/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.

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
9.2(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

```
Dell#debug ipv6 ospf packet
OSPFv3 packet related debugging is on for all interfaces
05:21:01 : OSPFv3: Sending, Ver:3, Type:1(Hello), Len:40, Router
ID:223.255.255.254, Area ID:0, Inst:0, on Po 255
05:21:03 : OSPFv3: Received, Ver:3, Type:1(Hello), Len:40, Router
ID:223.255.255.255, Area ID:0, Chksum:a177, Inst:0, from Vl 100
05:20:25 : OSPFv3: Sending, Ver:3, Type:4(LS Update), Len:580, Router
ID:223.255.255.254, Area ID:0, Inst:0, on Vl 1000
07:21:40 : OSPFv3: Received, Ver:3, Type:1(Hello), Len:40, Router ID:
223.255.255.254, Area ID:0, Chksum:af8f, Inst:0, from Te 1/6/1
Dell#
```

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 • 7 - external LSA • 8 - link-state advertisement (OSPFv3) • 9 - link local LSA (OSPFv2), Intra-Area-Prefix LSA (OSPFv3) • 11 - grace LSA (OSPFv3)



Lines Beginning With or Including	Description
Length:	Displays the packet length.
Router ID:	Displays the OSPF3 router ID.
Area ID:	Displays the Area ID.
Chksum:	Displays the OSPF3 checksum.

default-information originate

Configure the Dell Networking OS to generate a default external route into an OSPFv3 routing domain.

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 <code>always</code> to specify that default route information must always be advertised.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number to configure a metric value for the route. The range is from 1 to 16777214.
metric-type <i>type-value</i>	(OPTIONAL) Enter the keywords <code>metric-type</code> 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 <i>map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> 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
9.1.(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.

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.

Syntax	<code>graceful-restart grace-period seconds</code> To disable OSPFv3 graceful restart, enter <code>no graceful-restart grace-period</code> .	
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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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

Version	Description
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 <code>ipv6 router ospf</code> command to enter OSPFv3 configuration mode and then configure a grace period using the <code>graceful-restart grace-period</code> 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 <code>ipv6 ospf graceful-restart helper-reject</code> 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.

Syntax	<code>graceful-restart mode {planned-only unplanned-only}</code> To disable graceful restart mode, enter <code>no graceful-restart mode</code> .	
Parameters	planned-only	(OPTIONAL) Enter the keywords <code>planned-only</code> 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
91.(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 ospf area

Enable IPv6 OSPF on an interface.

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

<i>process-id</i>	Enter the process identification number.
<i>area area-id</i>	Specify the OSPF area. The range is from 0 to 65535.

Defaults none

Command Modes INTERFACE

Command History

Version	Description
91.(0.0)	Introduced on the S4810 and Z9000.
8.3.19.0	Introduced on the S4820T.



Version	Description
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.

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
9.1.(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 cost

Explicitly specify the cost of sending a packet on an interface.

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
9.1.(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:

$10^8 / \text{bandwidth}$

Using this formula, the default path cost is calculated as:

- GigabitEthernet—Default cost is 1
- TenGigabitEthernet—Default cost is 1
- FortygigEthernet — Default cost is 1
- Ethernet—Default cost is 10



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.

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
9.1.(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.

Syntax `ipv6 ospf encryption {null | ipsec spi number esp encryption-algorithm [key-encryption-type] key authentication-algorithm [key-encryption-type] key} }`

Parameters

<i>null</i>	Causes an encryption policy configured for the area to not be inherited on the interface.
<i>ipsec spi number</i>	Security Policy index (SPI) value that identifies an IPsec security policy. The range is from 256 to 4294967295.
<i>esp encryption-algorithm</i>	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
9.1.(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.

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
9.1.(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.

Syntax `ipv6 ospf hello-interval seconds`
To return to the default time interval, enter `no ipv6 ospf hello-interval`.



Parameters	<i>seconds</i>	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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.1.(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr><tr><td>7.8.1.0</td><td>Added support for the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr></table>		Version	Description	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.
Version	Description											
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.

Syntax	<code>ipv6 ospf priority <i>number</i></code> To return to the default time interval, use the <code>no ipv6 ospf priority</code> command.											
Parameters	<i>number</i>	Enter the number as the priority. The range is from 1 to 255.										
Defaults	1											
Command Modes	INTERFACE											
Command History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>91.(0.0)</td><td>Introduced on the S4810 and Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>7.8.1.0</td><td>Added support for the C-Series.</td></tr><tr><td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr></table>		Version	Description	91.(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.
Version	Description											
91.(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.

Syntax	<pre>ipv6 router ospf process-id [vrf vrf-name]</pre> To exit OSPF for IPv6, use the <code>no ipv6 router ospf process-id</code> command.	
Parameters	process-id	Enter the process identification number. The range is from 1 to 65535.
	vrf vrf-name	(Optional) Enter the keyword <code>vrf</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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

Version	Description
9.7(0.0)	Added support for VRF.
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.

maximum-paths

Enable the software to forward packets over multiple paths.

Syntax	<pre>maximum-paths number</pre> To disable packet forwarding over multiple paths, use the <code>no maximum-paths</code> 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	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	Added support for 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.

max-metric router-lsa

Configure the maximum cost of 65535 on a new router so that it functions as a stub router in the network and OSPF traffic destined to other networks is not forwarded on a path through the router.

C-Series, E-Series, Z-Series, S4810

Syntax **max-metric router-lsa** [**on-startup** {*announce-time* | **wait-for-bgp** [*wait-time*]}]

To remove the maximum metric assignment from an OSPF router and send LSAs with the currently configured cost, enter **no max-metric router-lsa** [**on-startup** {*announce-time* | **wait-for-bgp** [*wait-time*]}].

Parameters	on-startup <i>announce-time</i>	Enter the time (in seconds) following boot-up during which the maximum cost (65535) for transmitting OSPF traffic on router interfaces is announced in LSAs and the router functions as a stub router. Range: 5 to 86400 seconds.
	on-startup wait-for-bgp [<i>wait-time</i>]	Enable the router to announce the maximum metric in OSPF LSAs until the BGP routing table converges with updated routes. Default: 600 seconds. You can also specify the time (in seconds) that the router waits for the BGP routing table to converge before it stops advertising the maximum cost in LSAs and advertises the router's currently configured OSPF cost. Range: 5 to 86400 seconds.

Defaults Not Configured.

Command Modes ROUTER OSPF

Command History	Version 9.1.(0.0)	Introduced on the S4810 and Z9000.
	Version 8.4.2.5	Introduced on C-Series and E-Series TeraScale.
	Version 8.4.1.3	Introduced on E-Series ExaScale.

Usage Information When you bring a new router onto an OSPF network, you can configure the router to function as a stub router by globally reconfiguring the OSPF link cost so that other routers do not use a path that forwards



traffic destined to other networks through the new router for a specified time until the router's switching and routing functions are up and running, and the routing tables in network routers have converged.

By using the **max-metric router-lsa** command, you force the link cost of all OSPF non-stub links to the maximum link cost (65535). The advertisement of this maximum metric causes other routers to assign a cost to the new router that is higher than the cost of using an alternate path. Because of the high cost assigned to paths that pass through the new router, other routers will not use a path through the router as a transit path to forward traffic to other networks.

Use the **max-metric router-lsa** command to gracefully shut down or reload a router without dropping packets destined for other networks.



NOTE: If you enter the **max-metric router-lsa** command without an option (**on-startup announce-time** or **on-startup wait-for-bgp [wait-time]**), the maximum metric of 65535 is always announced in LSAs sent by the router.

Example

max-metric router-lsa

```
Dell(conf)#router ospf 10
Dell(conf-router_ospf)#log-adjacency-changes
Dell(conf-router_ospf)#network 4.1.1.0/24 area 0
Dell(conf-router_ospf)#network 1.1.1.0/24 area 1
Dell(conf-router_ospf)#max-metric router-lsa on-startup wait-for-bgp
Dell(conf-router_ospf)#exit

Dell(conf)#show ip ospf
Routing Process ospf 10 with ID 100.1.1.1 Virtual router default-vrf
Supports only single TOS (TOS0) routes
It is an Area Border Router
Originating router lsas with maximum metric
Time remaining 00:07:07
Condition : On-Startup while BGP is converging for 600 secs. State : Active
SPF schedule delay 5 secs, Hold time between two SPFs 10 secs
Convergence Level 0
Min LSA origination 5 secs, Min LSA arrival 1 secs
Number of area in this router is 2, normal 2 stub 0 nssa 0
  Area BACKBONE (0)
    Number of interface in this area is 1
    SPF algorithm executed 3 times
    Area ranges are
  Area 1
    Number of interface in this area is 1
    SPF algorithm executed 3 times
    Area ranges are

Dell(conf)#show ip ospf database router
Exception Flag: Announcing maximum link costs
  LS age: 198
  Options: (No TOS-capability, DC)
  LS Type: Router Links
  Link State ID: 2.1.1.1
  Advertising Router: 2.1.1.1
  LS Seq Number: 80000005
  Checksum: 0x9F5D
  Length: 48
  Number of Links: 2
```

passive-interface

Disable (suppress) sending routing updates on an interface.

Syntax `passive-interface interface`
To enable sending routing updates on an interface, use the `no passive-interface interface` command.

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number information:
	- For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a VLAN interface, enter the keyword <code>vlan</code> 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	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.
	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.

On configuring suppression using the `passive-interface` command, the state of the OSPF neighbor does not change to INIT; instead, the state of the OSPF neighbor changes to DOWN after the dead-timer expires.



redistribute

Redistribute into OSPFv3.

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 <code>bgp</code> then the autonomous system number. The range is from 1 to 65535.
connected	Enter the keyword <code>connected</code> to redistribute routes from physically connected interfaces.
static	Enter the keyword <code>static</code> to redistribute manually configured routes.
metric metric-value	Enter the keyword <code>metric</code> then the metric value. The range is from 0 to 16777214. The default is 20 .
metric-type type-value	(OPTIONAL) Enter the keywords <code>metric-type</code> 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 <code>route-map</code> 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 <code>tag</code> 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
9.1.(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.

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
9.1.(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 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.

Syntax **show crypto ipsec policy** [*name name*]

Parameters **name name** (OPTIONAL) Displays configuration details about a specified policy.

Defaults No default behavior or values.

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
9.1.(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.

Related Commands [show crypto ipsec sa ipv6](#)– displays the IPsec security associations used on OSPFv3 interfaces.

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 policy Command Fields

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	The encapsulating security payload (ESP) security policy index (SPI) for inbound and outbound links.
Outbound ESP SPI	
Inbound ESP Auth Key	The ESP authentication key for inbound and outbound links.
Outbound ESP Auth Key	
Inbound ESP Cipher Key	The ESP encryption key for inbound and outbound links.
Outbound ESP Cipher Key	
Transform set	The set of security protocols and algorithms used in the policy.
Inbound AH SPI	The authentication header (AH) security policy index (SPI) for inbound and outbound links.
Outbound AH SPI	
Inbound AH Key	The AH key for inbound and outbound links.
Outbound AH Key	

show crypto ipsec sa ipv6

Display the IPsec security associations (SAs) used on OSPFv3 interfaces.

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 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.
 - For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

No default behavior or values.

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
91.(0.0)	Introduced on the S4810 and Z9000.
84.2.0	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.

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 1/1/1
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 1/2/1
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 crypto ipsec sa ipv6 Command Fields

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.
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.

show ipv6 ospf database

Display information in the OSPFv3 database, including link-state advertisements (LSAs).

Syntax `show ipv6 ospf [process-number] [vrf vrf-name] database [database-summary | grace-lsa]`



Parameters	<i>process-number</i>	Enter the OSPF process number.
	<i>vrf vrf-name</i>	(Optional) Enter the keyword <i>vrf</i> 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.	
	<i>database-summary</i>	(OPTIONAL) Enter the keywords <i>database-summary</i> to view a summary of database LSA information.
	<i>grace-lsa</i>	(OPTIONAL): Enter the keywords <i>grace-lsa</i> to display the Type-11 Grace LSAs sent and received on an OSPFv3 router.
Defaults	none	
Command Modes	EXEC	
	EXEC Privilege	
Command History	Version	Description
	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 TeraScale routers.
	8.3.19.0	Introduced on the S4820T.
	7.8.1.0	Added support for C-Series.
Usage Information	The <code>show crypto ipsec sa ipv6</code> command output displays security associations set up for OSPFv3 links in IPsec authentication and encryption policies on the router.	
Related Commands	<code>show crypto ipsec policy</code> – displays the configuration of IPsec authentication and encryption policies.	
Example (grace-lsa)	<pre> Dell#show ipv6 ospf 3 database grace-lsa ! Type-11 Grace LSA (Area 0) LS Age : 10 Link State ID : 6.16.192.66 Advertising Router : 100.1.1.1 LS Seq Number : 0x80000001 Checksum : 0x1DF1 Length : 36 Associated Interface : Te 1/3/1 Restart Interval : 180 Restart Reason : Switch to Redundant Processor </pre>	
Example (database-summary)	<pre> Dell#show ipv6 ospf 3 database database-summary OSPFv3 Router with ID (1.1.1.1) (Process ID 1) </pre>	



```

Process 1 database summary
Type          Count/Status
Oper Status   1
Admin Status   1
Area Bdr Rtr Status   1
AS Bdr Rtr Status   1
AS Scope LSA Count   0
AS Scope LSA Cksum sum   0
Originate New LSAS   50
Rx New LSAS      22
Ext LSA Count     0
Rte Max Eq Cost Paths   10
GR grace-period   180
GR mode          planned and unplanned

Area 0 database summary
Type          Count/Status
Brd Rtr Count    1
AS Bdr Rtr Count   1
LSA count        6
Rtr LSA Count     2
Net LSA Count     1
Inter Area Pfx LSA Count 1
Inter Area Rtr LSA Count   0
Group Mem LSA Count   0
Type-7 LSA count     0
Intra Area Pfx LSA Count   2
Intra Area TE LSA Count   2

Area 1 database summary
Type          Count/Status
Brd Rtr Count    1
AS Bdr Rtr Count   1
LSA count        8
Rtr LSA Count     1
Net LSA Count     0
Inter Area Pfx LSA Count   5
Inter Area Rtr LSA Count   0
Group Mem LSA Count   0
Type-7 LSA count     0
Intra Area Pfx LSA Count   2
Intra Area TE LSA Count   2
E1200-T2C2#sh ipv6 ospf neighbor

Neighbor ID      Pri      State          Dead Time      Interface ID
Interface
63.114.8.36      1      FULL/DR        00:00:37       4 Te 1/4/1

```

show ipv6 ospf interface

View OSPFv3 interface information.

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 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.

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/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.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults none

Command Modes EXEC

Command History

Version	Description
9.2(1.0)	Introduced on the Z9500.
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 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#
```

show ipv6 ospf neighbor

Display the OSPF neighbor information on a per-interface basis.

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 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.
- For a VLAN interface, enter the keyword `vlan` then a number from 1 to 4094.

Defaults

none

Command Modes

EXEC

EXEC Privilege

Command History

Version

Description

9.7(0.0)

Added support for VRF.

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.

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		Te 1/2/1

```
Dell#
```

timers spf

Set the time interval between when the switch receives a topology change and starts a shortest path first (SPF) calculation.

S6000-ON

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 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
9.8(0.0)	Introduced on the S6000-ON, S6000, S4820T, S4810, S5000.

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)#ipv6 router ospf 1
Dell(conf-ipv6-router_ospf)#timer spf 2 5
Dell(conf-ipv6-router_ospf)#
Dell(conf-ipv6-router_ospf)#show config
!
ipv6 router ospf 1
timers spf 2 5
Dell(conf-ipv6-router_ospf)#
Dell(conf-ipv6-router_ospf)#end
Dell#
```



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.**

description

Add a description to this redirect list.

Syntax	<code>description {<i>description</i>}</code> To remove the description, use the <code>no description {<i>description</i>}</code> command.													
Parameters	<i>description</i>	Enter a description to identify the IP redirect list (16 characters maximum).												
Defaults	none													
Command Modes	REDIRECT-LIST													
Command History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.4(0.0)</td><td>Introduced on the S4810, S4820T, S6000, and Z9000.</td></tr><tr><td>8.4.2.1</td><td>Introduced on the C-Series and S-Series.</td></tr><tr><td>8.4.2.0</td><td>Introduced on the E-Series Tera Scale.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr></table>		Version	Description	9.7(0.0)	Introduced on the S6000-ON.	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 Tera Scale.	7.7.1.0	Introduced on the E-Series ExaScale.
Version	Description													
9.7(0.0)	Introduced on the S6000-ON.													
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 Tera Scale.													
7.7.1.0	Introduced on the E-Series ExaScale.													
Related Commands	ip redirect-list – enables an 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.

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 (conf-if-vl-)

Command History	
Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 Tera Scale.
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 includes the next-hop IP address where the incoming traffic is to be 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.

Syntax `ip redirect-list redirect-list-name`
To remove a redirect list, use the `no ip redirect-list` command.



Parameters	<i>redirect-list-name</i>	Enter the name of a redirect list.
Defaults	None	
Command Modes	CONFIGURATION	
Command History		
	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	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 Tera Scale.
	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.

Syntax	<pre>permit {ip-protocol-number protocol-type} {source mask any host ip-address} {destination mask any host ip-address} [bit] [operators]</pre> To remove the rule, use one of the following: • If you know the filter sequence number, use the <code>no seq sequence-number syntax</code> command. • You can also use the <code>no permit {ip-protocol-number protocol-type} {source mask any host ip-address} {destination mask any host ip-address} [bit] [operators]</code> command.	

Parameters	<i>ip-protocol-number</i>	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
	<i>protocol-type</i>	Enter one of the following keywords as the protocol type: • <code>icmp</code> for internet control message protocol • <code>ip</code> for any internet protocol • <code>tcp</code> for transmission control protocol • <code>udp</code> for user datagram protocol
	<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
	<i>mask</i>	Enter a network mask in /prefix format (/x).
	<i>any</i>	Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.
	<i>host ip-address</i>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
	<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
	<i>bit</i>	(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)
- `push` = 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 `portcommand` parameter.)

Defaults	none
Command Modes	REDIRECT-LIST
Command History	

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 Tera Scale.
7.7.1.0	Introduced on the E-Series ExaScale.

redirect

Configure a rule for the redirect list.

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.



<i>ip-address</i>	Enter the IP address of the forwarding router.
<i>slot/port</i>	Enter the keyword <code>slot / port</code> followed by the slot/port information.
<i>tunnel</i>	Enter the keyword <code>tunnel</code> to configure the tunnel setting.
<i>tunnel-id</i>	Enter the keyword <code>tunnel-id</code> to redirect the traffic.
<i>track</i>	Enter the keyword <code>track</code> to enable the tracking.
<i>track <obj-id></i>	Enter the keyword <code>track <obj-id></code> to track object-id.
<i>ip-protocol-number</i>	Enter a number from 0 to 255 for the protocol identified in the IP protocol header.
<i>protocol-type</i>	Enter one of the following keywords as the protocol type: • <code>icmp</code> for internet control message protocol • <code>ip</code> for any internet protocol • <code>tcp</code> for transmission control protocol • <code>udp</code> for user datagram protocol
<i>bit</i>	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: • <code>ack</code> = acknowledgement • <code>fin</code> = finish (no more data from the user) • <code>psh</code> = push function • <code>rst</code> = reset the connection • <code>syn</code> = synchronize sequence number • <code>urg</code> = urgent field
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	Enter a network mask in /prefix format (/x).
<i>any</i>	Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.
<i>host ip-address</i>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>operator</i>	(OPTIONAL) For TCP and UDP parameters only. Enter one of the following logical operand: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the <code>port</code> command parameter.)

Defaults	none
Command Modes	REDIRECT-LIST
Command History	
Version	Description
9.7(0.0)	Introduced on the S6000-ON.



Version	Description
9.7(0.0)	Added support for the track-id on the S4810, S4820T, S6000, and Z9000.
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 Tera Scale.
7.7.1.0	Introduced on the E-Series ExaScale.

seq

Configure a filter with an assigned sequence number for the redirect list.

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

<i>sequence-number</i>	Enter a number from 1 to 65535.
<i>permit</i>	Enter the keyword <code>permit</code> assign the sequence to the permit list.
<i>redirect</i>	Enter the keyword <code>redirect</code> to assign the sequence to the redirect list.
<i>ip-address</i>	Enter the keyword <code>IP</code> address of the forwarding router.
<i>tunnel</i>	Enter the keyword <code>tunnel</code> to configure the tunnel setting.
<i>tunnel-id</i>	Enter the keyword <code>tunnel-id</code> to redirect the traffic.
<i>track</i>	Enter the keyword <code>track</code> to enable the tracking.
<i>track <obj-id></i>	Enter the keyword <code>track <obj-id></code> to track object-id.
<i>ip-protocol-number</i>	Enter the keyword <code>ip-protocol-number</code> then the number from 0 to 255 for the protocol identified in the IP protocol header.
<i>protocol-type</i>	Enter one of the following keywords as the protocol type: • <code>icmp</code> for internet control message protocol • <code>ip</code> for any internet protocol • <code>tcp</code> for transmission control protocol • <code>udp</code> for user datagram protocol
<i>source</i>	Enter the IP address of the network or host from which the packets were sent.
<i>mask</i>	Enter a network mask in /prefix format (/x).
<i>any</i>	Enter the keyword <code>any</code> to specify that all traffic is subject to the filter.



host <i>ip-address</i>	Enter the keyword <code>host</code> then the IP address to specify a host IP address.
<i>destination</i>	Enter the IP address of the network or host to which the packets are sent.
<i>bit</i>	(OPTIONAL) For the TCP protocol type only, enter one or a combination of the following TCP flags: • <code>ack</code> = acknowledgement • <code>fin</code> = finish (no more data from the user) • <code>psh</code> = push function • <code>rst</code> = reset the connection • <code>syn</code> = synchronize sequence number • <code>urg</code> = urgent field
<i>operator</i>	(OPTIONAL) For the TCP and UDP parameters only. Enter one of the following logical operand: • <code>eq</code> = equal to • <code>neq</code> = not equal to • <code>gt</code> = greater than • <code>lt</code> = less than • <code>range</code> = inclusive range of ports (you must specify two ports for the port command parameter.)
<i>source port</i>	Enter the keywords <code>source-port</code> then the port number to be matched in the ACL rule in the ICAP rule
<i>destination-port</i>	Enter the keywords <code>destination-port</code> then the port number to be matched in the ACL rule in the ICAP rule.
<i>source-port-range</i>	Enter the keywords <code>Source-port-range</code> then the range of the start port to end port to be matched in the ACL rule in the ICAP rule.
<i>destination-port-range</i>	Enter the keywords <code>destination-port-range</code> 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
9.7(0.0)	Introduced on the S6000-ON.
9.7(0.0)	Added support for the track-id on the S4810, S4820T, S6000, and Z9000.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.



show cam pbr

Display the PBR CAM content.

Syntax `show cam pbr {[interface interface] | stack-unit slot-number port-set number]} [summary]`

Parameters

- interface *interface*** Enter the keyword `interface` then the name of the interface.
- stack-unit *number*** Enter the keyword `stack-unit` then the slot number.
- 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

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Usage Information The `show cam pbr` command displays the PBR CAM content.

Example

```
Dell#show cam pbr stack-unit 1 port-set 0
TCP Flag: Bit 5 - URG, Bit 4 - ACK, Bit 3 - PSH, Bit 2 - RST, Bit 1 - SYN, Bit 0 - FIN
Cam   Port VlanID Proto Tcp   Src   Dst   SrcIp                               DstIp
Index                                Flag  Port  Port
-----
00000 5      N/A      IP    0x0   0     0     22.22.2.22/32                      33.33.3.0/
00001 5      N/A      145   0x0   0     0     0.0.0.0/0                          44.4.4.4/3
00002 5      N/A      TCP   0x0   0     0     55.1.3.0/24                        66.6.6.6/3
00003 5      N/A      UDP   0x0   0     0     55.1.3.0/24                        66.6.6.6/3
00004 5      N/A      IP    0x0   0     0     0.0.0.0/0                          0.0.0.0/0
100)
Dell#
```

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.

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

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S4810, S4820T, S6000, and Z9000.

Example

```
Dell#show ip redirect-list explicit_tunnel
IP redirect-list explicit_tunnel:
Defined as:
seq 5 redirect tunnel 1 track 1 tcp 155.55.2.0/24 222.22.2.0/24, Track 1 [up],
Next-hop reachable (via Te 1/32/1)
seq 10 redirect tunnel 1 track 1 tcp any any, Track 1 [up], Next-hop reachable
(via Te 1/32/1)
seq 15 redirect tunnel 2 udp 155.55.0.0/16 host 144.144.144.144, Track 1 [up],
Next-hop reachable (via Te 1/32/1)
seq 35 redirect 155.1.1.2 track 5 ip 7.7.7.0/24 8.8.8.0/24, Track 5 [up], Next-
hop reachable (via Po 5)
seq 30 redirect 155.1.1.2 track 6 icmp host 8.8.8.8 any, Track 5 [up], Next-hop
reachable (via Po 5)
seq 35 redirect 42.1.1.2 icmp host 8.8.8.8 any, Next-hop reachable (via Vl 20)
seq 40 redirect 43.1.1.2 tcp 155.55.2.0/24 222.22.2.0/24, Next-hop reachable (via
Vl 30)
seq 45 redirect 31.1.1.2 track 200 ip 12.0.0.0 255.0.0.197 13.0.0.0 255.0.0.197,
Track 200 [up], Next-hop reachable (via Te 1/32/1)

Track 200 [up], Next-hop reachable (via Vl 20)
Track 200 [up], Next-hop reachable (via Po 5)
Track 200 [up], Next-hop reachable (via Po 7)
Track 200 [up], Next-hop reachable (via Te 2/18/1)
Track 200 [up], Next-hop reachable (via Te 2/19/1)
```



PIM-Sparse Mode (PIM-SM)

The protocol-independent multicast (PIM) commands are supported by the Dell Networking operating software on the platform.

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.

Syntax	<code>clear ip pim [vrf vrf-name] rp-mapping [rp-address]</code>	
Parameters	vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> 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.	
	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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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

Version	Description
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.
8.3.11.1	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.

Syntax `clear ip pim [vrf vrf-name] tib [group]`

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 (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, refer to the relevant *Dell 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)	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.
8.3.11.1	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.

Syntax

```
debug ip pim [vrf vrf-name] [bsr | events | group | packet [in | out] |  
register | state | timer [assert | hello | joinprune | register]]
```

To disable PIM debugging, use the `no debug ip pim [vrf vrf-name]` command or use the `undebug all` to disable all debugging command.

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> 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 <code>bsr</code> to view PIM Candidate RP/BSR activities.
events	(OPTIONAL) Enter the keyword <code>group</code> to view PIM messages for a specific group.
group	(OPTIONAL) Enter the keyword <code>group</code> to view PIM messages for a specific group.
packet [in out]	(OPTIONAL) Enter the keyword <code>packet</code> to view PIM packets. Enter one of the optional parameters: • <code>in</code>: to view incoming packets • <code>out</code>: to view outgoing packets
register	(OPTIONAL) Enter the keyword <code>register</code> to view PIM register address in dotted decimal format (A.B.C.D).
state	(OPTIONAL) Enter the keyword <code>state</code> to view PIM state changes.
timer [assert hello joinprune register]	(OPTIONAL) Enter the keyword <code>timer</code> to view PIM timers. Enter one of the optional parameters: • <code>assert</code>: to view the assertion timer • <code>hello</code>: to view the PIM neighbor keepalive timer • <code>joinprune</code>: to view the expiry timer (join/prune timer) • <code>register</code>: 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, refer to the relevant *Dell 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)	Added support for VRF. Introduced on the S6000-ON.



Version	Description
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.
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.

Syntax	<code>ip pim bsr-border</code> To return to the default value, use the <code>no ip pim bsr-border</code> command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 <code>clear ip pim rp-mapping</code> command.

ip pim bsr-candidate

To join the Bootstrap election process, configure the PIM router.

Syntax	<code>ip pim [vrf vrf-name] bsr-candidate interface [hash-mask-length] [priority]</code> To return to the default value, use the <code>no ip pim bsr-candidate [vrf vrf-name]</code> command.



Parameters	vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> followed by 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 <code>loopback</code> then a number from 0 to 16383. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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

Version	Description
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.
8.3.11.1	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	Added support for the VLAN interface.

ip pim dr-priority

Change the designated router (DR) priority for the interface.

Syntax	<code>ip pim dr-priority priority-value</code> To remove the DR priority value assigned, use the <code>no ip pim dr-priority</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 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.

Syntax	<code>ip pim [vrf vrf-name] join-filter ext-access-list</code> To remove the access list, use the <code>no ip pim [vrf vrf-name] join-filter ext-access-list</code> command.

Parameters	vrf vrf-name (OPTIONAL) Enter the keyword <code>vrf</code> 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
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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

Version	Description
9.7(0.0)	Removed the in and out parameters. Introduced on the S6000-ON.



Version	Description
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 C-Series for the port-channels and the S-Series.
7.7.1.0	Introduced on the E-Series.

Example

```
Dell(config)# 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
```

Related Commands [ip access-list extended](#) — configure an access list based on IP addresses or protocols.

ip pim neighbor-filter

To prevent a router from participating in protocol independent multicast (PIM), configure this feature.

Syntax

```
ip pim [vrf vrf-name] neighbor-filter {access-list}
```

To remove the restriction, use the `no ip pim [vrf vrf-name] neighbor-filter {access-list}` command.

Parameters

vrf vrf-name (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to prevent that VRF from participating in PIM.



NOTE: Applies to specific VRF if input is provided, else applies to default VRF.

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, refer to the relevant *Dell 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)	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.



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 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.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.

Syntax `ip pim [vrf vrf-name] register-filter access-list`



To return to the default, use the `no ip pim [vrf vrf-name] register-filter access-list` command.

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF.  NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.
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
9.7(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.
8.3.11.1	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

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.

Syntax

```
ip pim [vrf vrf-name] rp-address address {group-address group-address mask} [override]
```

To remove an RP address, use the `no ip pim [vrf vrf-name] rp-address address {group-address group-address mask} [override]` command.

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF.  NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.
address	Enter the RP address in dotted decimal format (A.B.C.D).



group-address <i>group-address</i> <i>mask</i>	Enter the keywords <code>group-address</code> then a group-address mask, in dotted decimal format (/xx), to assign that group address to the RP.
override	Enter the keyword <code>override</code> 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
9.7(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.
8.3.11.1	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. The RP is chosen based on a longer prefix match for a group. The RP selection does not depend on dynamic or static RP assignments.

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.

Syntax `ip pim [vrf vrf-name] rp-candidate {interface [priority]}`
To return to the default value, use the `no ip 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 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 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 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**.

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)	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.
8.3.11.1	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.

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

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



Version	Description
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 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 sparse-mode sg-expiry-timer

Enable expiry timers globally for all sources.

Syntax `ip pim [vrf vrf-name] sparse-mode sg-expiry-timer seconds`
To disable configured timers and return to default mode, use the `no ip pim [vrf vrf-name] sparse-mode sg-expiry-timer` command.

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> 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, refer to the relevant *Dell 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)	Added support for VRF. Removed the <code>acl-access-list</code> parameter. Modified the max value of S, G entry second range from 86400 to 65535. 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.

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 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.

ip pim ssm-range

Specify the SSM group range using an access list.

Syntax `ip pim [vrf vrf-name] ssm-range {access_list_name}`

Parameters

vrf vrf-name (OPTIONAL) Enter the keyword `vrf` followed by the name of the VRF to specify the SSM group range for that VRF.



NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.

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

Version	Description
9.7(0.0)	Introduced on the S6000-ON. Added support for VRF on S6000, S4810, S4820T, Z9000, Z9500, and S6000-ON.
9.5(0.1)	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.
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.

ip pim spt-threshold

To switch to the shortest path tree when the traffic reaches the specified threshold value, configure the PIM router.

Syntax

```
ip pim [vrf vrf-name] spt-threshold [infinity]
```

To return to the default value, use the `no ip pim [vrf vrf-name] spt-threshold [infinity]` command.

Parameters

vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to configure the PIM router on that VRF.

 **NOTE: Applies to specific VRF if input is provided, else applies to Default VRF.**

infinity	(OPTIONAL) Enter the keyword <code>infinity</code> 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
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.



Version	Description
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).

show ip pim bsr-router

View information on the Bootstrap router.

S6000-ON

Syntax `show ip pim [vrf vrf-name] 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
9.7(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.
8.3.11.1	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 interface

View information on the interfaces with IP PIM enabled.

S6000-ON

Syntax `show ip pim [vrf vrf-name] interface`

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
9.7(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.
8.1.1.0	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 <code>ip pim query-interval</code> command).
DR Prio	Displays the Designated Router priority value configured on the interface (use the <code>ip pim dr-priority</code> 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
165.87.34.5  Te 1/10/1 v2/S   0     30     1      165.87.34.5
10.1.1.2     Vl 10     v2/S   1     30     1      10.1.1.2
20.1.1.5     Vl 20     v2/S   1     30     1      20.1.1.5
165.87.31.200 Vl 30     v2/S   1     30     1      165.87.31.201
```



show ip pim neighbor

View PIM neighbors.

S6000-ON

Syntax `show ip pim [vrf vrf-name] neighbor`

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
9.7(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.
8.1.1.0	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 <code>ip pim dr-priority</code> 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 1/16/1    09:44:58/00:01:24 v2    1 / S
Dell#

```

show ip pim rp

View all multicast groups-to-RP mappings.

S6000-ON

Syntax `show ip pim [vrf vrf-name] rp [mapping | group-address]`

Parameters

vrf <i>vrf-name</i>	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the name of the VRF to configure this setting on that VRF.
mapping	(OPTIONAL) Enter the keyword <code>mapping</code> to display the multicast groups-to-RP mapping and information on how RP is learnt.
<i>group-address</i>	(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
97(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.
8.1.1.0	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 ssm-range

Display the non-default groups added using the SSM range feature.

S6000-ON

Syntax show ip pim [vrf vrf-name] ssm-range

Defaults none

Command Modes

- EXEC
- EXEC Privilege

Command History

Version	Description
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.

Exmaple Group Address / MaskLen

show ip pim summary

View information about PIM-SM operation.

S6000-ON

Syntax show ip pim [vrf vrf-name] 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
9.7(0.0)	Added support for VRF. Introduced on the S6000-ON.
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.
8.4.1.1	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).

S6000-ON

Syntax `show ip 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 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 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, refer to the relevant *Dell 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)	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.
8.1.1.0	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



Field	Description
	• 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
```



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.

 **NOTE: The monitoring port should not be a part of any other configuration.**

description

Enter a description of this monitoring session.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-7.7.1.0	Introduced on the E-Series.

Related Commands [monitor session](#) — enables a monitoring session.

monitor multicast-queue

Configure monitor QoS multicast queue ID.

Syntax `monitor multicast-queue queue-id`
To remove the configuration, use the `no monitor multicast-queue` command.

Parameters `queue-id` Enter the QoS multicast queue ID. The range is from 0 to 9.

Defaults `queue-id: 0`
Enable status: Disabled

Command Modes CONFIGURATION

Example `Dell(conf)#monitor multicast-queue 7`

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

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

Version	Description
9.8(0.0)	Introduced on the S6000, Z9500, S6000-ON.

Related Commands [show running-config monitor session](#) — displays information about monitor configurations.



monitor session

Create a session for monitoring traffic with port monitoring.

Syntax `monitor session session-ID [type { rpm | erpm [set ip dscp dscp_value | set ip ttl ttl_value]]] [drop]`

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

<i>session-ID</i>	Enter a session identification number. The range is from 0 to 65535.
type	Specifies one of the following type: · rpm · erpm
rpm	Creates a remote port monitoring (rpm) session.
erpm	Creates an encapsulated remote port monitoring (erpm) session.
set ip dscp	Configures the Differentiated Services Code Point (DSCP) value of the packets in the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic. To revert to the default value, use the no form of this command.
<i>dscp_value</i>	DSCP value of the packets in the ERSPAN traffic. The range is from 0 to 63. The default value is 0.
set ip ttl	Configures the IP time-to-live (TTL) value of the Encapsulated Remote Switched Port Analyzer (ERSPAN) traffic. To revert to the default configuration, use the no form of this command.
<i>ttl_value</i>	IP TTL value of the ERSPAN traffic. The range is from 1 to 255. The default value is 255.
drop	Monitors only the dropped packets in the Ingress.

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
9.8(0.0)	Added the drop parameter.
9.7(0.0)	Introduced on the S6000-ON. Introduced the <code>set ip dscp</code> and <code>set ip ttl</code> parameters.
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.



Version	Description
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.

Example

```
Dell#show monitor session
      SessID  Source      Destination      Dir  Mode  Source IP
Dest IP      DSCP    TTL
-----
0      Te 1/12/1      remote-ip      rx   Flow 1.1.1.1
7.1.1.2      0      255
0      Po 1      remote-ip      tx   Flow 1.1.1.1
7.1.1.2      0      255
1      Vl 11      remote-ip      rx   Flow 5.1.1.1
3.1.1.2      0      255
```

Related Command [show monitor session](#) — displays the monitor session.

[show running-config monitor session](#) — displays the running configuration of a monitor session.

rate-limit

Configure the rate-limit to limit the mirrored packets.

Syntax `rate-limit limit`

To remove the limit, use the `no rate-limit limit` command.

Parameters **limit** Enter the rate-limit value. The range is from 0 to 40000 Megabits per second.

Defaults 60

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
9.8(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, Z9500.

Related Commands [monitor session](#) — enables a monitoring session.

[show monitor session](#) — displays the monitor session.



show config

Display the current monitor session configuration.

Syntax	<code>show config</code>
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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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-1) #show config
!
monitor session 1
source TenGigabitEthernet 1/1/1 destination Port-channel 1 direction rx
```

show monitor session

Display information about monitoring sessions.

Syntax	<code>show monitor session {session-ID}</code> To display monitoring information for all sessions, use the <code>show monitor session</code> command.	
Parameters	session-ID	(OPTIONAL) Enter a session identification number. The range is 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
9.7(0.0)	Introduced on the S6000-ON.
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 Source IP Dest IP DSCP TTL
-----
1 Te 1/2/1 remote-ip rx Port 0.0.0.0 0.0.0.0 0 0
Dell#show monitor session
SessID Source Destination Dir Mode Source IP Dest IP DSCP TTL
-----
1 Te 1/2/1 remote-ip rx Port 0.0.0.0 0.0.0.0 0 255
99 NONE NONE N/A N/A N/A N/A N/A N/A
```

Related Commands [monitor session](#) — creates a monitoring session.

[rate-limit](#) — configures the rate-limit.

show running-config monitor session

Display the running configuration of all monitor sessions or a specific session.

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
9.7(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 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# show running-config monitor session
!
monitor session 1
source TenGigabitEthernet 1/1/1 destination TenGigabitEthernet 1/2
direction rx
!
monitor multicast-queue 7
```

Related Commands [monitor session](#) — creates a monitoring session.

[show monitor session](#) — displays a monitoring session.

source (port monitoring)

Configure a port monitor source.

Syntax

```
source {interface | range | any} 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 one of the following keywords and 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 VLAN interface enter the keyword `VLAN` followed by a number from 1 to 4094.
- For a port channel interface, enter the keywords `port-channel` then a number.

range Enter the keyword `range` to specify the list of interfaces.

any Enter the keyword `any` to specify all interfaces.



NOTE: This option is applicable only with drop monitor session.

destination Enter the keyword `destination` to specify the destination interface.

- 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.

interface Enter one of the following keywords and 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 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.

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, refer to the relevant *Dell Networking OS Command Line Reference Guide*.

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

Version	Description
9.8(0.0)	Added the any parameter.
9.7(0.0)	Introduced on the S6000-ON.
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.

Version	Description
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.

Example

```
Dell# monitor session 0
source Port-channel 10 destination TenGigabitEthernet 1/33/1 direction tx
```



Private VLAN (PVLAN)

The private VLAN (PVLAN) feature of the Dell Networking operating software is supported on the platforms.

Private VLANs extend the Dell Networking OS 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 Dell Networking OS private VLAN implementation is based on RFC 3069.

For more information, refer to the following commands. The command output is augmented in 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).

ip local-proxy-arp

Enable/disable Layer 3 communication between secondary VLANs in a private VLAN.

S6000-ON

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` (use `no ip-local-proxy-arp`) in a secondary VLAN, Layer 3 communication may happen between some secondary VLAN hosts, until the address resolution protocol (ARP) timeout happens on those secondary VLAN 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, refer to the relevant *Dell 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.
9.0.2.0	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.

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.

[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.

S6000-ON

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 <code>community</code> to set the VLAN as a community VLAN.
isolated	Enter the keyword <code>isolated</code> to configure the VLAN as an isolated VLAN.
primary	Enter the keyword <code>primary</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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.

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 indicates this.)
- 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.
[switchport mode private-vlan](#) — sets PVLAN mode of the selected port.



private-vlan mapping secondary-vlan

Map secondary VLANs to the selected primary VLAN.

S6000-ON

Syntax	<code>[no] private-vlan mapping secondary-vlan <i>vlan-list</i></code> To remove specific secondary VLANs from the configuration, use the <code>no private-vlan mapping secondary-vlan <i>vlan-list</i></code> command syntax.															
Parameters	<i>vlan-list</i>	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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.8.1.0</td><td>Introduced on the C-Series and S-Series.</td></tr></table>		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.	7.8.1.0	Introduced on the C-Series and S-Series.
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.															
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. switchport mode private-vlan — sets PVLAN mode of the selected port.															



switchport mode private-vlan

Set PVLAN mode of the selected port.

S6000-ON

Syntax	<code>[no] switchport mode private-vlan {host promiscuous trunk}</code> To remove PVLAN mode from the selected port, use the <code>no switchport mode private-vlan</code> command.	
Parameters	host	Enter the keyword <code>host</code> to configure the selected port or port channel as an isolated interface in a PVLAN.
	promiscuous	Enter the keyword <code>promiscuous</code> to configure the selected port or port channel as an promiscuous interface.
	trunk	Enter the keyword <code>trunk</code> 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

Usage Information	The assignment of the various PVLAN port types to port and port channel (LAG) interfaces is shown in the following example.

Example	<pre>Dell#conf Dell(conf)#interface TenGigabitEthernet 2/1/1 Dell(conf-if-te-2/1/1)#switchport mode private-vlan promiscuous Dell(conf)#interface TenGigabitEthernet 2/2/1 Dell(conf-if-te-2/2/1)#switchport mode private-vlan host Dell(conf)#interface TenGigabitEthernet 2/3/1 Dell(conf-if-te-2/3/1)#switchport mode private-vlan trunk Dell(conf)#interface port-channel 10 Dell(conf-if-te-2/3/1)#switchport mode private-vlan promiscuous</pre>



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.



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.

Dell Networking OS supports PVST+ on the S6000–ON platform.

 **NOTE:** For easier command line entry, the plus (+) sign is not used at the command line.

description

Enter a description of the PVST+.

S6000–ON

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
9.7(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.
pre- 7.7.1.1	Introduced.

Related Commands

[protocol spanning-tree pvst](#) — enter SPANNING TREE mode on the switch.

disable

Disable PVST+ globally.

S6000-ON

Syntax	<code>disable</code> To enable PVST+, use the <code>no disable</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
pre- 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.

S6000-ON

Syntax	<code>extend system-id</code>
Defaults	Disabled
Command Modes	PROTOCOL PVST
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

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 1/10/1 128.140 128   200000 FWD 0    32773 0001.e832.73f7 128.140
Te 1/12/1 128.142 128   200000 DIS 0    32773 0001.e832.73f7 128.142

Interface
Name      Role PortID  Prio  Cost   Sts Cost Link-type Edge
-----
Te 1/10/1  Desg 128.140 128   200000 FWD 0    P2P      No
Te 1/12/1  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.

S6000-ON

Syntax	<pre>protocol spanning-tree pvst</pre> To disable PVST+, use the <code>disable</code> command.
Defaults	none
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. 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.
9.0.2.0	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.
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.

S6000-ON

Syntax `show spanning-tree pvst [vlan vlan-id] [brief] [guard]`

Parameters

vlan <i>vlan-id</i>	(OPTIONAL) Enter the keyword <code>vlan</code> then the VLAN ID. The range is 1 to 4094.
brief	(OPTIONAL) Enter the keyword <code>brief</code> to view a synopsis of the PVST+ configuration information.
<i>interface</i>	(OPTIONAL) Enter one of the interface keywords along with the slot/port information: - For a Port Channel interface, enter the keyword <code>port-channel</code> then a number: The range is 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information.



- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

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
9.7(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.
8.5.1.0	Added support for 4-port 40G line cards on ExaScale.
8.4.2.1	Support for the optional <code>guard</code> 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).

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 1/0/1	128.130	128	20000	FWD	20000	4096 0001.e801.6aa8	128.426	
Te 1/1/1	128.131	128	20000	BLK	20000	4096 0001.e801.6aa8	128.427	
Te 1/16/1	128.146	128	20000	FWD	20000	16384 0001.e805.e306	128.146	
Te 1/17/1	128.147	128	20000	FWD	20000	16384 0001.e805.e306	128.147	

Interface								
Name	Role	PortID	Prio	Cost	Sts	Cost	Link-type	Edge
Te 1/2/1	Root	128.130	128	20000	FWD	20000	P2P	No
Te 1/1/1	Altr	128.131	128	20000	BLK	20000	P2P	No
Te 1/16/1	Desg	128.146	128	20000	FWD	20000	P2P	Yes
Te 1/17/1	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 occurred 00:57:00

Port 130 (TenGigabitEthernet 1/2/1) 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 1/1/1) 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 1/16/1) 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 1/17/1) 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 1/1/1

TenGigabitEthernet 1/1/1 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 1/1/1  128.1223 128   20000 EDS 0 32768 0001.e800.a12b 128.1223
```

Example (EDS/ PVID)

```
Dell#show spanning-tree pvst vlan 2 interface tengigabitethernet 1/1/1

TenGigabitEthernet 1/1/1 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 1/1/1  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 1/1/1  5          INCON(Root) Rootguard
Te 1/2/1  5          FWD          Loopguard
Te 1/3/1  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.

S6000-ON

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 <code>edge-port</code> to configure the interface as a PVST+ edge port.
bpduguard	Enter the keyword <code>portfast</code> to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword <code>bpduguard</code> to disable the port when it receives a BPDU.
shutdown-on-violation	(OPTIONAL) Enter the keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.



err-disable	Enter the keywords <code>err-disable</code> to enable the port to be put into the error-disable state (EDS) if an error condition occurs.
vlan <i>vlan-range</i>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
cost <i>number</i>	Enter the keyword <code>cost</code> then the port cost value. The range is from 1 to 200000. Defaults: • 100 Mb/s Ethernet interface = 200000. • 1-Gigabit Ethernet interface = 20000. • 10-Gigabit Ethernet interface = 2000. • Port Channel interface with one 100 Mb/s Ethernet = 200000. • Port Channel interface with one 1 Gigabit Ethernet = 20000. • Port Channel interface with one 10 Gigabit Ethernet = 2000. • Port Channel with two 1 Gigabit Ethernet = 18000. • Port Channel with two 10 Gigabit Ethernet = 1800. • Port Channel with two 100 Mbps Ethernet = 180000.
priority <i>value</i>	Enter the keyword <code>priority</code> then the Port priority value in increments of 16. The range is from 0 to 240. The default is 128 .
loopguard	(C-, S-, and E-Series TeraScale only) Enter the keyword <code>loopguard</code> to enable loop guard on a PVST+ port or port-channel interface.
rootguard	(C-, S-, and E-Series TeraScale only) Enter the keyword <code>rootguard</code> 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, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Introduced the <code>loopguard</code> and <code>rootguard</code> 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 <code>shutdown-on-violation</code> 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.

Example

```
Dell(conf-if-te-1/1/1)#spanning-tree pvst vlan 3 cost 1800
Dell(conf-if-te-1/1/1)#end
Dell(conf-if-te-1/1/1)#/lshow config
!
interface TenGigabitEthernet 1/1/1
  no ip address
  switchport
  spanning-tree pvst vlan 3 cost 18000
  no shutdown
Dell(conf-if-te-1/1/1)#end
Dell#
```

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.

S6000-ON

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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

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, Dell Networking OS places the port in the Error-Disable state. This behavior might result in the network not converging. To prevent Dell Networking OS from executing this action, use the <code>no spanning-tree pvst err-disable</code> command cause <code>invalid-pvst-bpdu</code>.

Related Commands	show spanning-tree pvst — views the PVST+ configuration.

tc-flush-standard

Enable the MAC address flushing after receiving every topology change notification.

S6000-ON

Syntax	<code>tc-flush-standard</code> To disable, use the <code>no tc-flush-standard</code> command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.



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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.5.1.0	Introduced.

Usage Information By default, Dell Networking OS 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.

S6000-ON

Syntax `vlan vlan-range bridge-priority value`
To return to the default value, use the `no vlan bridge-priority` command.

Parameters

vlan <i>vlan-range</i>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
bridge-priority <i>value</i>	Enter the keywords <code>bridge-priority</code> 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
9.7(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.



Version	Description
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced.

Related Commands [vlan forward-delay](#) — changes the time interval before Dell Networking OS 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.

S6000-ON

Syntax `vlan vlan-range forward-delay seconds`
To return to the default setting, use the `no vlan forward-delay` command.

Parameters

vlan <i>vlan-range</i>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
forward-delay <i>seconds</i>	Enter the keywords <code>forward-delay</code> then the time interval, in seconds, that Dell Networking OS 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
9.7(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.



Version	Description
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.

S6000-ON

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
9.7(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.
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.

S6000-ON

Syntax `vlan vlan-range max-age seconds`
 To return to the default, use the `no vlan max-age` command.

Parameters

vlan <i>vlan-range</i>	Enter the keyword <code>vlan</code> then the VLAN numbers. The range is from 1 to 4094.
max-age <i>seconds</i>	Enter the keywords <code>max-age</code> then the time interval, in seconds, that Dell Networking OS 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
9.7(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.
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 hello-time](#) — changes the time interval between BPDUs.

[show spanning-tree pvst](#) — displays the PVST+ configuration.



Quality of Service (QoS)

The Dell Networking operating software commands for quality of service (QoS) include traffic conditioning and congestion control. QoS commands are not universally supported on all Dell Networking Products. platform.

This chapter contains the following sections:

- [Global Configuration Commands](#)
- [Per-Port QoS Commands](#)
- [Policy-Based QoS Commands](#)

Global Configuration Commands

There is only one global configuration QoS command.

qos-rate-adjust

By default, while rate limiting, policing, and shaping, Dell Networking OS 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. You can optionally include overhead fields in rate metering calculations by enabling QoS Rate Adjustment.

S6000-ON

Syntax	<code>qos-rate-adjustment <i>overhead-bytes</i></code>	
Parameters	<i>overhead-bytes</i>	Include a specified 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	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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
8.3.1.0	Introduced.

service-class bandwidth-percentage

Specify a minimum bandwidth for queues.

S6000-ON

Syntax	<code>service-class bandwidth-percentage queue0 <i>number</i> queue1 <i>number</i> queue2 <i>number</i> queue3 <i>number</i></code>	
Parameters	<i>number</i>	Enter the bandwidth-weight, as a percentage.
Defaults	none	
Command Modes	CONFIGURATION	
Command History	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.
	8.3.7.1	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 <code>service-class bandwidth-percentage</code> command from CONFIGURATION mode. The command is applied in the same way as the <code>bandwidth-percentage</code> command in an output QoS policy. The <code>bandwidth-percentage</code> command in QOS-POLICY-OUT mode supersedes the <code>service-class bandwidth-percentage</code> command.	

service-class dot1p-mapping

Configure a service-class criterion based on a dot1p value.

S6000-ON

Syntax	<code>service-class dot1p-mapping {dot1p0 <i>queue</i> dot1p1 <i>queue</i> dot1p2 <i>queue</i> dot1p3 <i>queue</i> dot1p4 <i>queue</i> dot1p5 <i>queue</i> dot1p6 <i>queue</i> dot1p7 <i>queue</i>}</code>	
Parameters	<i>queue</i>	Enter a value 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 : 2 0 1 3 4 5 6 7	
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.
9.0.2.0	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 To apply dot1p-queue-mapping, use the `service-class dynamic dot1p` command.

Related Commands [show qos dot1p-queue-mapping](#) — displays the dot1p priority to queue mapping on the switch.

show qos dot1p-queue-mapping

Displays the dot1p priority to queue mapping on the switch.

Syntax `show qos dot1p-queue-mapping`

Defaults

- dot1p Priority: 0 1 2 3 4 5 6 7
- Queue: 2 0 1 3 4 5 6 7

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
9.7(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.

Usage Information `trust dot1p`, `do1p-priority`, `service-class dynamic dot1`; all these features work over the mapping in this command output.

Related Commands [service-class dot1p-mapping](#) — Identifies the class map.

strict-priority queue

Configure a unicast queue as a strict-priority (SP) queue.

S6000-ON

Syntax `strict-priority queue unicast number`



Parameters	unicast <i>number</i> Enter the keyword <code>unicast</code> then the queue number. The range is from 1 to 3.												
Defaults	none												
Command Modes	CONFIGURATION												
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> </table>	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.
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.												
Usage Information	After you configure a unicast queue as strict-priority, that particular queue, on the entire chassis, is treated as a <code>strict-priority</code> queue. Traffic for a strict priority is scheduled before any other queues are serviced. For example, if you send 100% line rate traffic over the SP queue, it starves all other queues on the ports on which this traffic is flowing.												

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.

Syntax	<code>dot1p-priority <i>priority-value</i></code> To delete the IEEE 802.1p configuration on the interface, use the <code>no dot1p-priority</code> command.						
Defaults	none						
Command Modes	INTERFACE						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. Version The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> </table>	Version	Description	9.7(0.0)	Introduced on the S6000-ON.	9.0.2.0	Introduced on the S6000.
Version	Description						
9.7(0.0)	Introduced on the S6000-ON.						
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.
7.5.1.0	Introduced on the C-Series.
pre- 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.

S6000-ON

Syntax `rate police [kbps] committed-rate [burst-KB] [peak [kbps] peak-rate [burst-KB]] [vlan vlan-id]`

Parameters

kbps	Enter the keyword <code>kbps</code> to specify the rate limit in Kilobits per second (Kbps). 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 50 .
peak peak-rate	(OPTIONAL) Enter the keyword <code>peak</code> then a number to specify the peak rate in Mbps. The range is from 0 to 40000.
vlan vlan-id	(OPTIONAL) Enter the keyword <code>vlan</code> then a VLAN ID to police traffic to those specific VLANs. The range is from 1 to 4094.

Defaults Granularity for `committed-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
9.7(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.

Usage Information



NOTE: Per Port rate police is supported for Layer 2 tagged and untagged switched traffic and for Layer 3 traffic. Per VLAN rate police is supported on only tagged ports with Layer 2 switched traffic.

S-Series

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.

rate shape

Shape the traffic output on the selected interface.

S6000-ON

Syntax `rate shape [kbps] rate [burst-KB]`

Parameters

kbps	Enter the keyword <code>kbps</code> to specify the rate limit in Kilobits per second (Kbps). On S-Series, make the value a multiple of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
rate	The range is from 10 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
9.7(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.

Usage Information On 40-port 10G stack-unit if the traffic is shaped between 64 and 1000 Kbs, for some values, the shaped rate is much less than the value configured.



NOTE: When packets of size greater than 7000 bytes are expected to be received from the network, Dell Networking recommends that you configure the burst value to be more than 175 KB if you configured the rate shape. Such a setting ensures proper bandwidth sharing across queues.

Related Commands [rate-shape](#) — shapes traffic output as part of the designated policy.

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.

S6000-ON

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:

dot1p	Queue ID
0	2
1	0
2	1
3	3
4	4
5	5
6	6
7	7

Command Modes

- INTERFACE
- 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.
9.0.2.0	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 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.

Policy-Based QoS Commands

Policy-based traffic classification is handled with class maps. These maps classify unicast traffic into one of eight classes in S-Series or eight classes in case of S6000. Dell Networking OS enables 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.

S6000-ON

Syntax `bandwidth-percentage percentage`
To remove the bandwidth percentage, use the `no bandwidth-percentage` command.

Parameters *percentage* Enter the percentage assignment of bandwidth 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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
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. This utility is supported on the S6000 platform.

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 mode

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
Version 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.

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/access a class map. Class maps differentiate traffic so that you can apply separate quality-of-service policies to each class.

S6000-ON

Syntax `class-map {match-all | match-any} class-map-name [cpu-qos] [layer2]`

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 <code>match-any</code> 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).
cpu-qos	Enter the keyword <code>cpu-qos</code> to assign this Class Map to control plane traffic only (CoPP).
layer2	Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is Layer 3 .

Defaults Layer 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
9.7(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	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.

Related Commands [ip access-list extended](#) — configures an extended IP ACL.

[ip access-list standard](#) — configures a standard 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 qos statistics clears statistics from show qos statistics.

S6000—ON

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/subport 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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.18.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

Related Commands [show qos statistics](#) — displays the QoS statistics.

description

Add a description to the selected policy map or QoS policy.

S6000—ON

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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>pre- 7.7.1.0</td><td>Introduced.</td></tr> </tbody> </table>	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.	pre- 7.7.1.0	Introduced.
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.														
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).

 **NOTE: IPv6 class-maps and IP-any class-maps do not match. This condition is true for IPv6 and IP-any class-maps on both ACLs as well as VLANs.**

S6000-ON

Syntax

```
match ip access-group access-group-name [set-ip-dscp value | set-color value]
```

To remove ACL match criteria from a class map, use the `no match ip access-group access-group-name [set-ip-dscp value | set-color 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.

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
9.7(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.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

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.

S6000-ON

Syntax `match {ip | ipv6 | ip-any} dscp dscp-list [set-ip-dscp 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]` command.

Parameters

ip	Enter the keyword <code>ip</code> to support IPv4 traffic.
ipv6	Enter the keyword <code>ipv6</code> to support IPv6 traffic.
ip-any	Enter the keyword <code>ip-any</code> 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 <code>set-ip-dscp</code> 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
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Added the ipv6 and ip-any options on the Z9000, S6000, S4820T, S4810, MXL.
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 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 DSCP 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.

S6000-ON

Syntax

```
match {ip | ipv6 | ip-any} precedence ip-precedence-list [set-ip-dscp 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]` command.

Parameters

ip	Enter the keyword <code>ip</code> to support IPv4 traffic.
ipv6	Enter the keyword <code>ipv6</code> to support IPv6 traffic.
ip-any	Enter the keyword <code>ip-any</code> 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 <code>set-ip-dscp</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.3.11.1	Introduced on the Z9000.
8.3.7.0	Introduced on the S4810.

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 mac access-group

Configure a match criterion for a class map, based on the contents of the designated MAC ACL.

S6000-ON

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
9.7(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.

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.

S6000-ON

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
9.7(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.

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.

S6000-ON

Syntax `match mac vlan number`



Parameters	<i>number</i>	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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>8.2.1.0</td><td>Introduced.</td></tr></table>		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.
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.															
Usage Information	To access this command, enter the <code>class-map</code> 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 (output) applied on an interface.

S6000-ON

Syntax	<code>policy-aggregate <i>qos-policy-name</i></code> To remove a policy aggregate configuration, use the <code>no policy-aggregate <i>qos-policy-name</i></code> command.	
Parameters	<i>qos-policy-name</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> . 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.
	9.0.2.0	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.

Usage Information If the rate shape exists in both aggregate and per-queue qos-policy, minimum of 2 take effect. Some of all Queue-rate will not exceed aggregate.

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.

S6000-ON

Syntax `policy-map-input policy-map-name cpu-qos | [layer2]`
To remove an input policy map, use the `no policy-map-input policy-map-name cpu-qos | [layer2]` command.

Parameters

<i>policy-map-name</i>	Enter the name of the <code>policy map</code> in character format (32 characters maximum).
<i>cpu-qos</i>	Enter the <code>cpu-qos</code> keyword to assign this ACL to control plane traffic only.
<i>layer2</i>	(OPTIONAL) Enter the keyword <code>layer2</code> to specify a Layer 2 Class Map. The default is Layer 3 .

Defaults **Layer 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
9.7(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.

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`).

Related Commands [service-queue](#) — assigns a class map and QoS policy to different queues.
[service-policy input](#) — applies an input policy map to the selected interface.



policy-map-output

Create an output policy map.

S6000-ON

Syntax	<code>policy-map-output <i>policy-map-name</i></code> To remove a policy map, use the <code>no policy-map-output <i>policy-map-name</i></code> command.													
Parameters	<i>policy-map-name</i>	Enter the name for the policy map in character format (32 characters maximum).												
Defaults	none													
Command Modes	CONFIGURATION													
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.													
	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr></table>	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.	
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.													
Usage Information	To assign traffic to different flows using QoS policy, use the Output Policy map. This command enables Policy-Map-Output Configuration mode (<code>conf-policy-map-out</code>).													
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.

S6000-ON

Syntax	<code>qos-policy-input <i>qos-policy-name</i> cpu-qos layer2</code> To remove an existing input QoS policy from the router, use the <code>no qos-policy-input <i>qos-policy-name</i> cpu-qos layer2</code> command.	
Parameters	<i>qos-policy-name</i>	Enter the name for the policy map in character format (32 characters maximum).
	cpu-qos	(OPTIONAL) Enter the keyword <code>cpu-qos</code> keyword to assign this ACL to control plane traffic only.



layer2 (OPTIONAL) Enter the keyword `layer2` to specify a Layer 2 Class Map. The default is **Layer 3**.

Defaults **Layer 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
9.7(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.

Usage Information Use this command to specify the name of the input QoS policy. Once input policy is specified, rate-police can be defined. This command enables the 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.

Related Commands [rate police](#) — incoming traffic policing function.

qos-policy-output

Create a QoS output policy.

S6000-ON

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

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



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 Use this command to specify the name of the output QoS policy. Once output policy is specified, rate-shape, scheduler strict, bandwidth-percentage, and WRED can be defined. This command enables the qos-policy-output configuration mode—(conf-qos-policy-out).

Related Commands [bandwidth-percentage](#) — assigns percentage of bandwidth to the class/queue.
[wred](#) — assigns yellow or green drop precedence.

rate-police

Specify the policing functionality on incoming traffic.

S6000-ON

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
9.7(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.

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 police](#) — specifies traffic policing on the selected interface.
[qos-policy-input](#) — creates a QoS output policy.

rate-shape

Shape traffic output as part of the designated policy.

S6000-ON

Syntax `rate-shape [kbps] rate [burst-KB]`

Parameters

kbps	Enter the keyword <code>kbps</code> 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).
rate	The range is from 10 to 40000.
burst-KB	(OPTIONAL) Enter the burst size in KB. The range is from 0 to 40000. The default is 100 .

Defaults Burst size is 10KB. Granularity for rate is Mbps unless you use the `kbps` option.

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
9.7(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.

Usage Information On 40-port 10G stack-unit if the 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.
[qos-policy-output](#) — creates a QoS output policy.



service-policy input

Apply an input policy map to the selected interface.

S6000-ON

Syntax	<pre>service-policy input <i>policy-map-name</i> [<i>layer2</i>]</pre> To remove the input policy map from the interface, use the <code>no service-policy input <i>policy-map-name</i> [<i>layer2</i>]</code> command.	
Parameters	<i>policy-map-name</i>	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.
	<i>layer2</i>	(OPTIONAL) Enter the keyword <code>layer2</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	
	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.
9.0.2.0	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	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 <code>service-policy</code> commands are not allowed on a port channel. The <code>service-policy input <i>policy-map-name</i></code> command and the <code>service-class dynamic dot1p</code> command are not allowed simultaneously 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.

S6000-ON

Syntax	<pre>service-policy output <i>policy-map-name</i></pre> To remove the output policy map from the interface, use the <code>no service-policy output <i>policy-map-name</i></code> command.



Parameters	<i>policy-map-name</i> 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> </tbody> </table>	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.
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.												
Usage Information	A single policy-map can be attached to one or more interfaces to specify the service-policy for those interfaces.												
Related Commands	policy-map-output — creates an output policy map.												

service-queue

Assign a class map and QoS policy to different queues.

S6000-ON

Syntax	<pre>service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]</pre> To remove the queue assignment, use the <code>no service-queue queue-id [class-map class-map-name] [qos-policy qos-policy-name]</code> command.
Parameters	<i>queue-id</i> Enter the value used to identify a queue. The range is from 0 to 7. <i>class-map class-map-name</i> (OPTIONAL) Enter the keyword <code>class-map</code> 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. <i>qos-policy qos-policy-name</i> (OPTIONAL) Enter the keywords <code>qos-policy</code> 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 <code>policy-map-input</code> and output QoS policy under <code>policy-map-output</code> 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
9.7(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.

Usage Information There are eight queues per interface on the S6000 and four queues on the S-Series. This command assigns a class map or QoS policy to different queues.

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.

S6000-ON

Syntax `set {ip-dscp value | mac-dot1p value}`

Parameters

ip-dscp <i>value</i>	(OPTIONAL) Enter the keywords <code>ip-dscp</code> then the IP DSCP value. The range is from 0 to 63.
mac-dot1p <i>value</i>	Enter the keywords <code>mac-dot1p</code> 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
9.7(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.



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.

S6000-ON

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
9.7(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.

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.

S6000-ON

Syntax `show qos policy-map {summary [interface] | detail}`

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/subport information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.



detail 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/subport 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
9.7(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.

Example (IPv4)

```
Dell#show qos policy-map detail tengigabitethernet 1/1/1

Interface TenGigabitEthernet 4/1/1

Policy-map-input policy
Queue# Class-map-name Qos-policy-name
0 - q0
1 CM1 q1
2 CM2 q2
3 CM3 q3
4 CM4 q4
5 CM5 q5
6 CM6 q6
7 CM7 q7
Dell#
```

Example (IPv6)

```
Dell# show qos policy-map detail Tegigabitethernet 1/1/1

Interface TeGigabitEthernet 4/1/1

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 4/1/1      PM1          -
Te 4/2/1      PM2          PMOut
Dell#
```

show qos policy-map-input

View the input QoS policy map details.

S6000-ON

Syntax

```
show qos policy-map-input [policy-map-name] [class class-map-name] [qos-
policy-input qos-policy-name]
```

Parameters

<i>policy-map-name</i>	Enter the policy map name.
<i>class class-map-name</i>	Enter the keyword <code>class</code> then the class map name.
<i>qos-policy-input qos-policy-name</i>	Enter the keyword <code>qos-policy-input</code> 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
9.7(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.

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#
```



show qos policy-map-output

View the output QoS policy map details.

S6000-ON

Syntax `show qos policy-map-output [policy-map-name] [qos-policy-output qos-policy-name]`

Parameters

<i>policy-map-name</i>	Enter the policy map name.
<i>qos-policy-output</i> <i>qos-policy-name</i>	Enter the keyword <code>qos-policy-output</code> 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
9.7(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.

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.

S6000-ON

Syntax `show qos qos-policy-input [qos-policy-name]`

Parameters

<i>qos-policy-name</i>	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
9.7(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.

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.

S6000-ON

Syntax `show qos qos-policy-output [qos-policy-name]`

Parameters

<i>qos-policy-name</i>	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
9.7(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.



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.

S6000-ON

Syntax

```
show qos statistics {egress-queue [interface]} | {wred-profile [interface]}
| [interface]
```

Parameters

egress-queue interface

Enter the keyword `egress-queue` to display the egress-queue statistics 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/subport information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

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/subport information.
- For a 40-Gigabit Ethernet interface, enter the keyword `fortyGigE` then the slot/port information.

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/subport 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
9.8(0.0)	Added the <code>egress-queue</code> keyword.
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.

Related Command [clear hardware stack-unit](#) - Clear statistics from selected hardware components.

show qos wred-profile

View the WRED profile details.

S6000-ON

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, refer to the relevant *Dell 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.
9.0.2.0	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.

Example

```
Dell#show qos wred-profile
Wred-profile-name  min-threshold  max-threshold  max-drop-rate
wred_drop          0              0              100
wred_teng_y         467            4671           100
wred_teng_g         467            4671           50
wred_fortyg_y       467            4671           50
wred_fortyg_g       467            4671           25
```

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 S6000 platform.



S6000-ON

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
<i>number</i>	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
9.7(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%



shared-threshold-weight on the queue	% of available shared buffer that can be consumed by the queue.
11	88.89%

Example

```
Dell(conf-if-te-1/8/1)#Service-class buffer shared-threshold-weight queue5
4 queue7 6
```

test cam-usage

Check the Input Policy Map configuration for the CAM usage.

S6000-ON

Syntax

```
test cam-usage service-policy input policy-map stack-unit {[number port-set
portpipe number] | [all]}
```

Parameters

<i>policy-map</i>	Enter the policy map name.
<i>stack-unitnumber</i>	(OPTIONAL) Enter the keyword <i>stack-unit</i> then the stack-unit slot number.
<i>port-set portpipe number</i>	Enter the keywords <i>port-set</i> then the stack-unit port pipe number. The range is from 0 or 1.
<i>stack-unit all</i>	(OPTIONAL) Enter the keywords <i>stack-unit</i> all to indicate all stack-unit.

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
9.7(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.

Usage Information

This feature allows you to determine if the CAM has enough space available before applying the configuration on an interface.

An input policy map with both Trust and Class-map configuration, the Class-map rules are ignored and only the Trust rule is programmed in the CAM. In such an instance, the Estimated CAM output column contains the size of the CAM space required for the Trust rule and not the Class-map rule.

The following describes the `test cam-usage service-policy input policy-map stack-unit` command shown in the following example.



Field	Description
stack-unit	Indicates the stack-unit slot number.
Portpipe	Indicates the portpipe number.
CAM Partition	The CAM space where the rules are added.
Available CAM	Indicates the free CAM space, in the partition, for the classification rules.
	 NOTE: The CAM entries reserved for the default rules are not included in the Available CAM column; free entries, from the default rules space, cannot be used as a policy map for the classification rules.
Estimated CAM per Port	Indicates the number of free CAM entries required (for the classification rules) to apply the input policy map on a single interface.
	 NOTE: The CAM entries for the default rule are not included in this column; a CAM entry for the default rule is always dedicated to a port and is always available for that interface.
Status (Allowed ports)	Indicates if the input policy map configuration on an interface belonging to a stack-unit/port-pipe is successful — Allowed (n) — or not successful — Exception. The allowed number (n) indicates the number of ports in that port-pipe on which the Policy Map can be applied successfully.
	 NOTE: In a Layer 2 Policy Map, IPv4/IPv6 rules are not allowed; therefore, the output contains only L2ACL CAM partition entries.

Example

```
Dell# test cam-usage service-policy input pmap_l2 stack-unit all
```

For a L2 Input Policy Map pmap_l2, the output must be as follows,

stack-unit	Portpipe	CAM Partition	Available CAM	Estimated CAM	Status
				per Port	(Allowed ports)
0	0	L2ACL	500	200	Allowed (2)
0	1	L2ACL	100	200	Exception
1	0	L2ACL	1000	200	Allowed (5)
1	1	L2ACL	0	200	Exception
		...			
		...			
		...			
13	1	L2ACL	400	200	Allowed (2)

```
Dell#
```

threshold

Specify the minimum and maximum threshold values for the configured WRED profiles.

S6000-ON

Syntax

```
threshold min number max number max-drop-probability
```

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 1 to 9360.



max-drop-probability number Enter the keyword **max-drop-probability** followed by the maximum number of packets for the WRED profile. The range is from 0 to 100 KB

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
9.7(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	Introduced on the S4810.

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.

Pre-Defined WRED Profile Name	Minimum Threshold	Maximum Threshold	Maximum 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

Related Commands [wred-profile](#) — creates a WRED profile.

trust

Specify dynamic classification (DSCP) or dot1p to trust.

S6000-ON

Syntax `trust {diffserv [fallback] | dot1p [fallback]}`

Parameters

diffserv	Enter the keyword <code>diffserv</code> to specify trust of DSCP markings.
dot1p	Enter the keyword <code>dot1p</code> to specify trust dot1p configuration.
fallback	Enter the keyword <code>fallback</code> to classify packets according to their DSCP or dot1p 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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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	When you configure <code>trust</code> , matched bytes/packets counters are not incremented in the <code>show qos statistics</code> command.

Dynamic mapping honors packets marked according to the standard definitions of DSCP. The following lists the default mapping.

DSCP/CP hex Range (XXX)	DSCP Definition	Traditional IP Precedence	S6000 Internal Queue ID	S-Series Internal Queue ID	DSCP/CP Decimal
111XXX		Network Control	7	3	48–63
110XXX		Internetwork Control	6	3	48–63
101XXX	EF (Expedited Forwarding)	CRITIC/ECP	5	2	32–47
100XXX	AF4 (Assured Forwarding)	Flash Override	4	2	32–47
011XXX	AF3	Flash	3	1	16–31
010XXX	AF2	Immediate	2	1	16–31
001XXX	AF1	Priority	1	0	0–15
000XXX	BE (Best Effort)	Best Effort	0	0	0–15

wred

Designate the WRED profile to yellow or green traffic.

S6000-ON

Syntax	<code>wred {yellow green} profile-name</code> To remove the WRED drop precedence, use the <code>no wred {yellow green} [profile-name]</code> command.



Parameters	yellow green	Enter the keyword <code>yellow</code> for yellow traffic. A DSCP value of xxx110 and xxx100, xxx101 maps to yellow. Enter the keyword <code>green</code> for green traffic. A DSCP value of xxx0xx are green and DSCP 11111 are red packets.
	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: <code>wred_drop</code> , <code>wred-ge_y</code> , <code>wred-ge_g</code> , <code>wred_teng_y</code> , <code>wred_teng_</code> .

Defaults When WRED green is applied, default WRED yellow profiles take effect and vice-versa.

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
9.7(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.

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 ecn

To indicate network congestion, rather than dropping packets, use explicit congestion notification (ECN).

S6000-ON

Syntax	<code>wred ecn</code>
	To stop marking packets, use the <code>no wred ecn</code> command.
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 <i>Dell Networking OS Command Line Reference Guide</i> .



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.
9.0.2.0	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 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 two 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 weight

Configure the weight factor for computation of average-queue size. This weight value applies to front-end ports. This mechanism to configure a weight for WRED and ECN functionality for front-end ports is supported on the S6000 and Z9000 platforms.

S6000-ON

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 ports only.
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
9.7(0.0)	Introduced on the S6000-ON.



Version	Description
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 FTOS (conf-qos-policy-out) # wred weight 5

wred-profile

Create a WRED profile and name the profile.

S6000-ON

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.
If green profile is applied, default yellow also take effect and vice-versa.

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.
9.0.2.0	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 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).

Related Commands [threshold](#) — specifies the minimum and maximum threshold values of the WRED profile.



rate shape

Define the rate-shaping method to be either as a measure of bytes or packets for each of the hierarchical QoS (HQoS) nodes at the leaf level to be applied to each queue.

S6000-ON

Syntax `[no] rate-shape [kbps | pps] peak-rate [burst-KB/Packets] [committed [kbps | pps] committed-rate [burst-KB/Packets]]`

Parameters

kbps	Enter the keyword kbps to specify the committed rate limit in Kilobits per second (Kbps). Specify this value as a multiple of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
pps	Enter the keyword pps to specify the committed rate limit in packets per second (pps). The range is from 1 to 268000000. The default granularity is Megabits per second (Mbps).
<i>committed-rate</i>	Define the committed rate, which is the guaranteed or minimum confirmed rate for the packets. Specify this value as a multiple of 64 if you specify the committed rate in Kbps. The range is from 0 to 40000000 for Kbps. The range is from 1 to 268000000 for pps. The range is from 0 to 40000 for Mbps (which is the default measure for rate limits if you do not explicitly configure Kbps or pps)
<i>burst-KB</i>	(OPTIONAL) Enter the committed burst size in KB. The range is from 0 to 10000. The default is 50 KB. The default peak burst is regarded as the same value as the configured committed burst size.
<i>Packets</i>	(OPTIONAL) Enter the committed burst size as a count of packets. The range is from 1 to 1073000. The default is 50 packets. The default peak rate is regarded as the same value as the configured committed rate.
<i>peak-rate</i>	Define the peak rate, which is the guaranteed or minimum confirmed rate for the packets. Specify this value as a multiple of 64 if you specify the peak rate in Kbps. The range is from 0 to 40000000 for Kbps. The range is from 1 to 268000000 for pps. The range is from 0 to 40000 for Mbps (which is the default measure for rate limits if you do not explicitly configure Kbps or pps)
kbps	Enter the keyword kbps to specify the peak rate limit in Kilobits per second (Kbps). Specify this value as a multiple of 64. The range is from 0 to 40000000. The default granularity is Megabits per second (Mbps).
pps	Enter the keyword pps to specify the peak rate limit in packets per second (pps). The range is from 1 to 268000000. The default granularity is Megabits per second (Mbps).
<i>peak-rate</i>	Define the peak rate, which is the guaranteed or minimum confirmed rate for the packets. Specify this value as a multiple of 64 if you specify the peak rate in Kbps. The range is from 0 to 40000000 for Kbps. The range is from 1 to 268000000 for pps. The range is from 0 to 40000 for Mbps (which is the default measure for rate limits if you do not explicitly configure Kbps or pps)
<i>burst-KB</i>	(OPTIONAL) Enter the peak burst size in KB. The range is from 0 to 10000. The default is 50 KB.
<i>Packets</i>	(OPTIONAL) Enter the peak burst size as a count of packets. The range is from 1 to 1073000. The default is 50 packets. The default peak rate is regarded as the same value as the configured peak rate.



Default	Granularity for rate is Mbps unless you use the kbps option.	
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.3(0.0)	Added support for committed rate and committed burst size, and for configuration of rate limits on the S6000 platform.
Usage Information	If you specify the pps keyword after the rate-shape command, the peak rate, peak burst, committed rate and committed burst are all considered to be values as a measure of packets. If you do not specify the pps or kbps keyword, the peak and committed rate settings are considered to be values in Mbps. Similarly, if you enter the kbps keyword, the peak and committed rate settings are treated as values in Kbps.	
	You cannot configure the committed rate settings to use a different metric or unit from the metric that is set for peak rate attributes because when you use the rate-shape kbps command, it denotes the metric for peak and committed rate attributes). Similarly, if you use the rate-shape pps option , it denotes the metric for peak rate and committed rate attributes.	
	If you attempt to define the committed rate to be less than the peak rate, an error message is displayed stating that the peak rate cannot be lower than the committed rate. You can configure all the rate shaping parameters to be either in bytes or packets measure for each queue. The rate and burst parameters for both minimum and maximum settings for a queue can be either in packets or bytes. You cannot configure some of rate shaping attributes to be in bytes measure and the remaining rate shaping attributes to be in packets measure; all the rate shaping attributes must contain the same metric or unit of measure.	
Example	Dell (conf-qos-policy-out) #rate-shape pps 100 100 peak pps 1000 200	
	Dell (conf-qos-policy-out) #rate-shape kbps 1024 100 peak kbps 102400 75	
	Dell (conf-qos-policy-out) # rate-shape 100 100 peak 1000 750	
	Dell(conf-qos-policy-in)#rate-police 100 25 peak 80 500 % Error: Peak rate cannot be less than committed rate.	

service-pool wred

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 S6000 and Z9000 platforms.

Create a global buffer pool that is a shared buffer pool accessed by multiple queues when the minimum guaranteed buffers for the queue are consumed. S4810, S4820T, S6000, and Z9000 platforms support 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 configuration 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.

Syntax	[No] service-pool wred {green weight yellow} {[pool0 number/string] [pool1 number/string]}	
Parameters	service-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
9.7(0.0)	Introduced on the S6000-ON.
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 pool, service0, is used for lossy queues and the pool, service1, is used for lossless (PFC) queues in all the platforms.

You can configure the weight for the WRED average queue size for service1 on the S6000 Switch, which is the only platform in which PFC is supported for this service pool. On the Z9000 Switch, only service0 can be configured because it 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 `service-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
```



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.

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 <code>yellow</code> 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 <code>red</code> keyword. Traffic marked as red is dropped.
dscp-list	Enter a list of IP DSCP values. The <code>dscp-list</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.5.0.0	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.

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.

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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><thead><tr><th>Version</th><th>Description</th></tr></thead><tbody><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>Version 9.5.0.0</td><td>Introduced on the Z9000, S6000, S4820T, S4810, and MXL.</td></tr></tbody></table>	Version	Description	9.7(0.0)	Introduced on the S6000-ON.	Version 9.5.0.0	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Version	Description						
9.7(0.0)	Introduced on the S6000-ON.						
Version 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 1/11/1. <pre>Dell(conf)# int te 1/11/1 Dell(conf-if-te-1/11/1)# qos dscp-color-policy bat-enclave-map</pre>						
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-policy

Display DSCP color policy configuration for one or all interfaces.

Syntax	<code>show qos dscp-color-policy {summary [<i>interface</i>] detail {<i>interface</i>}}</code>	
Parameters	summary Enter the <code>summary</code> keyword to display summary information about a color policy on one or more interfaces.	
	Detail Enter the <code>detail</code> keyword to display detailed information about a color policy on one or more interfaces.	
	interface Enter the name of the interface that has color policy configured.	
Defaults	None	
Command Modes	EXEC	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	



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.
9.5.0.0	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.

Example

Display summary information about a color policy on one or more interfaces.

```
Dell# show qos dscp-color-policy summary
```

```
Interface      dscp-color-map
TE 1/10/1      mapONE
TE 1/11/1      mapTWO
```

Display summary information about a color policy on a specific interface.

```
Dell# show qos dscp-color-policy summary te 1/10/1
Interface      dscp-color-map
TE 1/10/1      mapONE
```

Displayed detailed color policy information on an interface.

```
Dell# show qos dscp-color-policy detail te 1/10/1
Interface TenGigabitEthernet 1/10/1

Dscp-color-map mapONE
  yellow 4,7
  red 20,30
```

Related Commands — Displays DSCP color maps [show qos dscp-color-map](#)

show qos dscp-color-map

Display the DSCP color map for one or all interfaces.

Syntax `show qos dscp-color-map map-name`

Parameters

<i>map-name</i>	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
9.7(0.0)	Introduced on the S6000-ON.
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 [show qos dscp-color-policy](#) — Displaying a DSCP Color Policy Configuration



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) on the platform.

The Dell Networking OS 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*.

auto-summary

Restore the default behavior of automatic summarization of subnet routes into network routes. This command applies only to RIP version 2.

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
9.7(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.
7.6.1.0	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 Dell Networking OS routing table.

S6000-ON

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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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.

S6000-ON

Syntax `debug ip rip [interface | database | events [interface] | trigger]`
To turn off debugging output, use the `no debug ip rip` command.

Parameters

<i>interface</i>	(OPTIONAL) Enter the interface type and ID as one of the following:

- 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, enter the keyword `vlan` then a number from 1 to 4094.



database	(OPTIONAL) Enter the keyword <code>database</code> to display messages when there is a change to the RIP database.
events	(OPTIONAL) Enter the keyword <code>events</code> to debug only RIP protocol changes.
trigger	(OPTIONAL) Enter the keyword <code>trigger</code> 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
9.7(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.
8.5.1.0	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.
pre- 6.2.1.1	Introduced on the E-Series.

default-information originate

Generate a default route for the RIP traffic.

S6000-ON

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 <code>always</code> to enable the switch software to always advertise the default route.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number as the metric value. The range is from 1 to 16. The default is 1 .
route-map <i>map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> 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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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.

S6000-ON

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
9.7(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.
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.

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.

S6000-ON

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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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.

S6000-ON

Syntax	<code>distance weight [ip-address mask [prefix-name]]</code> To return to the default values, use the <code>no distance weight [ip-address mask]</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

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.

S6000-ON

Syntax	<code>distribute-list prefix-list-name in [interface]</code>



To delete the filter, use the `no distribute-list prefix-list-name in` command.

Parameters

<i>prefix-list-name</i>	Enter the name of a configured prefix list.
<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port as one of the following: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> 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
9.7(0.0)	Introduced on the S6000-ON.
9.2(1.0)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.
8.3.29.0	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.
pre- 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.

S6000-ON

Syntax

```
distribute-list prefix-list-name out [interface | bgp | connected | isis |  
ospf | static]
```



To delete the filter, use the `no distribute-list prefix-list-name out` command.

Parameters

<i>prefix-list-name</i>	Enter the name of a configured prefix list.
<i>interface</i>	(OPTIONAL) Identifies the interface type slot/port as one of the following: • For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN, enter the keyword <code>vlan</code> then a number from 1 to 4094.
<i>connected</i>	(OPTIONAL) Enter the keyword <code>connected</code> to filter only directly connected routes.
<i>isis</i>	(OPTIONAL) Enter the keyword <code>isis</code> to filter only IS-IS routes.
<i>ospf</i>	(OPTIONAL) Enter the keyword <code>ospf</code> to filter all OSPF routes.
<i>static</i>	(OPTIONAL) Enter the keyword <code>static</code> 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
9.7(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 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.
pre- 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.

S6000-ON

Syntax	<code>ip poison-reverse</code> To disable poison reverse, use the <code>no ip poison-reverse</code> command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . 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.
9.0.2.0	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.

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.

S6000-ON

Syntax	<code>ip rip receive version [1] [2]</code> To return to the default, use the <code>no ip rip receive version</code> 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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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.

S6000-ON

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 RIP version 1.
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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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.

S6000-ON

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
9.7(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.
7.6.1.0	Introduced on the C-Series.



Version	Description
pre- 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.

S6000-ON

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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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.

S6000-ON

Syntax `neighbor ip-address`



To delete a neighbor setting, use the `no neighbor ip-address` command.

Parameters	<i>ip-address</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

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 <code>passive-interface</code> command with the <code>neighbor</code> 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.

S6000-ON

Syntax	<code>network ip-address</code> To disable RIP for a network, use the <code>no network ip-address</code> command.
Parameters	<i>ip-address</i> 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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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.

S6000-ON

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

<i>prefix-list-name</i>	Enter the name of an established Prefix list to determine which incoming routes are modified.
<i>offset</i>	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.
<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port or number information: - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN, enter the keyword <code>vlan</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.2(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.
8.3.7.0	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.

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.

S6000-ON

Syntax	<code>output-delay delay</code> To return to the switch software defaults for interpacket delay, use the <code>no output-delay</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

Usage Information This command is intended for low-speed interfaces.

passive-interface

Suppress routing updates on a specified interface.

S6000-ON

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 128.
- 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 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
9.7(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 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.
pre- 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.

S6000-ON

Syntax `redistribute {connected | static}`
To disable redistribution, use the `no redistribute {connected | static}` command.

Parameters

connected	Enter the keyword <code>connected</code> to specify that information from active routes on interfaces is redistributed.
static	Enter the keyword <code>static</code> 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
9.7(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.
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.

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.

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 <code>level-1</code> to redistribute only IS-IS Level-1 routes.
level-1-2	(OPTIONAL) Enter the keywords <code>level-1-2</code> to redistribute both IS-IS Level-1 and Level-2 routes.
level-2	(OPTIONAL) Enter the keywords <code>level-2</code> to redistribute only IS-IS Level-2 routes.
metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number as the metric value. The range is from 0 to 16.
route-map <i>map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> 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 *FTOS Command Line Reference Guide*.

The following is a list of the FTOS version history for this command.

Version	Description
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.
pre- 6.2.1.1	Introduced on the E-Series.

redistribute ospf

Redistribute routing information from an OSPF process.

S6000-ON

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	<i>process-id</i>	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 <code>match external</code> 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 <code>match internal</code> to indicate that internal routes should be redistributed.
	metric <i>metric-value</i>	(OPTIONAL) Enter the keyword <code>metric</code> then a number as the metric value. The range is from 0 to 16.
	route-map <i>map-name</i>	(OPTIONAL) Enter the keywords <code>route-map</code> 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
9.7(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.



Version	Description
7.6.1.0	Introduced on the C-Series.
pre- 6.2.1.1	Introduced on the E-Series.

router rip

To configure and enable RIP, enter ROUTER RIP mode.

S6000-ON

Syntax	<pre>router rip</pre> To disable RIP, use the <code>no router rip</code> command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>.

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.
9.0.2.0	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.

Usage Information	To enable RIP, assign a network address using the <code>network</code> command.
Example	<pre>Dell(conf)#router rip Dell(conf-router_rip)#</pre>
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.

S6000-ON

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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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 1/1/1
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.

S6000-ON

Syntax `show ip rip database [ip-address mask]`

Parameters

<i>ip-address</i>	(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.
<i>mask</i>	(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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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, GigabitEthernet 1/15/1
204.250.54.0/24    auto-summary
203.250.49.0/24
    [50/1] via 192.13.1.3, 00:00:12, GigabitEthernet 1/14/1
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.

S6000-ON

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
9.7(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 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 GigabitEthernet 2/1/1
  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.

S6000-ON

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**.



<i>invalid</i>	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 .
<i>holddown</i>	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 .
<i>flush</i>	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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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.

S6000-ON

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 Dell Networking OS 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
9.7(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.
7.6.1.0	Introduced on the C-Series.
pre- 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.



Remote Monitoring (RMON)

The Dell Networking operating software remote monitoring (RMON) is implemented on the S6000-ON platform.

Dell Networking OS RMON is based on IEEE standards, providing both 32-bit and 64-bit monitoring and long-term statistics collection. Dell Networking OS 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; RFC-4502
- Probe Configuration (Capabilities, SoftwareRev, HardwareRev, DateTime and ResetControl); RFC-4502

Dell Networking OS 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.**

rmon alarm

Set an alarm on any MIB object.

S6000-ON

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.

<i>interval</i>	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.
<i>delta</i>	Enter the keyword <code>delta</code> to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
<i>absolute</i>	Enter the keyword <code>absolute</code> to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
<i>rising-threshold value event-number</i>	Enter the keywords <code>rising-threshold</code> 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.
<i>falling-threshold value event-number</i>	Enter the keywords <code>falling-threshold</code> 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.
<i>owner string</i>	(OPTIONAL) Enter the keyword <code>owner</code> 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
9.7(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.
6.1.1.0	Introduced on the E-Series.



rmon collection history

Enable the RMON MIB history group of statistics collection on an interface.

S6000-ON

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 <i>integer</i>	Enter the keyword <code>controlEntry</code> 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 <i>name</i>	(OPTIONAL) Enter the keyword <code>owner</code> then the owner name to record the owner of the RMON group of statistics.
buckets <i>number</i>	(OPTIONAL) Enter the keyword <code>buckets</code> 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 <i>seconds</i>	(OPTIONAL) Enter the keyword <code>interval</code> 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
9.7(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.
6.1.1.0	Introduced on the E-Series.



rmon collection statistics

Enable RMON MIB statistics collection on an interface.

S6000-ON

Syntax	<pre>rmon collection statistics {controlEntry integer} [owner name]</pre> To remove RMON MIB statistics collection on an interface, use the <code>no rmon collection statistics {controlEntry integer}</code> command.				
Parameters	<table><tr><td>controlEntry integer</td><td>Enter the keyword <code>controlEntry</code> 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.</td></tr><tr><td>owner name</td><td>(OPTIONAL) Enter the keyword <code>owner</code> then the owner name to record the owner of the RMON group of statistics.</td></tr></table>	controlEntry integer	Enter the keyword <code>controlEntry</code> 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 <code>owner</code> then the owner name to record the owner of the RMON group of statistics.
controlEntry integer	Enter the keyword <code>controlEntry</code> 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 <code>owner</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .				

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.
9.0.2.0	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.

rmon event

Add an event in the RMON event table.

S6000-ON

Syntax	<pre>rmon event number [log] [trap community] [description string]</pre> To disable RMON on an interface, use the <code>no rmon event number</code> command.



Parameters	<i>number</i>	Assign an event number in integer format. The range is from 1 to 65535. You must ensure that the value you enter is unique in the RMON event table.
	log	(OPTIONAL) Enter the keyword <code>log</code> to generate an RMON event log. This option sets the <code>eventType</code> to either <code>log</code> or <code>log-and-snmptrap</code> in the RMON event table. The default is <code>None</code> .
	trap <i>community</i>	(OPTIONAL) Enter the keyword <code>trap</code> followed by the SNMP community string to generate SNMP traps for an RMON event entry. This option sets the <code>eventType</code> to either <code>snmptrap</code> or <code>log-and-snmptrap</code> in the RMON event table. In addition to the SNMP traps, this option also generates a syslog.
	description <i>string</i>	(OPTIONAL) Enter the keyword <code>description</code> then a string describing the event.
	owner <i>name</i>	(OPTIONAL) Enter the keyword <code>owner</code> then the name of the owner of this event.
Defaults	As noted in the <i>Parameters</i> section.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

rmon hc-alarm

Set an alarm on any MIB object.

S6000-ON

Syntax	<pre>rmon hc-alarm <i>number</i> variable <i>interval</i> {delta absolute} rising-threshold value <i>event-number</i> falling-threshold value <i>event-number</i> [<i>owner string</i>]</pre> To disable the alarm, use the <code>no rmon hc-alarm <i>number</i></code> command.

Parameters	<i>number</i> Enter the alarm integer number from 1 to 65535. The value must be unique in the RMON alarm table.



<i>variable</i>	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.
<i>interval</i>	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.
<i>delta</i>	Enter the keyword <code>delta</code> to test the change between MIB variables. This is the alarmSampleType in the RMON alarm table.
<i>absolute</i>	Enter the keyword <code>absolute</code> to test each MIB variable directly. This is the alarmSampleType in the RMON alarm table.
<i>rising-threshold value event-number</i>	Enter the keywords <code>rising-threshold</code> 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.
<i>falling-threshold value event-number</i>	Enter the keywords <code>falling-threshold</code> 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.
<i>owner string</i>	(OPTIONAL) Enter the keyword <code>owner</code> 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
9.7(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.
6.1.1.0	Introduced on the E-Series.



show rmon

Display the RMON running status including the memory usage.

S6000-ON

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
9.7(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.
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.

S6000-ON

Syntax `show rmon alarms [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword <code>brief</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

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 alarm br
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
6          1.3.6.1.2.1.1.3
7          1.3.6.1.2.1.1.3
8          1.3.6.1.2.1.1.3
9          1.3.6.1.2.1.1.3
10         1.3.6.1.2.1.1.3
11         1.3.6.1.2.1.1.3
12         1.3.6.1.2.1.1.3
13         1.3.6.1.2.1.1.3
14         1.3.6.1.2.1.1.3
15         1.3.6.1.2.1.1.3
16         1.3.6.1.2.1.1.3
17         1.3.6.1.2.1.1.3
18         1.3.6.1.2.1.1.3
19         1.3.6.1.2.1.1.3
20         1.3.6.1.2.1.1.3
21         1.3.6.1.2.1.1.3
22         1.3.6.1.2.1.1.3
Dell#

```



show rmon events

Display the contents of the RMON event table.

S6000-ON

Syntax `show rmon events [index] [brief]`

Parameters

index	(OPTIONAL) Enter the table index number to display just that entry.
brief	(OPTIONAL) Enter the keyword <code>brief</code> 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
9.7(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.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell(conf)#rmon event 111          -> Default case
Dell(conf)#rmon event 112 log      -> Only "log" option
Dell(conf)#rmon event 113 trap private -> Only "trap" option
Dell(conf)#rmon event 114 log trap public-> Both "log" and "trap" options
Dell(conf)#do show rmon events
RMON event entry 111
  description:
  event type: none.
  event community:
  event last time sent: none
  event owner:
  event status: OK
RMON event entry 112
  description:
  event type: LOG.
  event community:
  event last time sent: none
  event owner:
  event status: OK
RMON event entry 113
  description:
  event type: SNMP TRAP.
  event community: private
  event last time sent: none
```



```

event owner:
event status: OK
RMON event entry 114
description:
event type: LOG and SNMP TRAP.
event community: public
event last time sent: none
event owner:
event status: OK

```

Example (Brief)

```

Dell#show rmon event brief
index      description
-----
1          1
2          2
3          3
4          4
5          5
6          6
7          7
8          8
9          9
10         10
11         11
12         12
13         13
14         14
15         15
16         16
17         17
18         18
19         19
20         20
21         21
22         22
Dell#

```

show rmon hc-alarm

Display the contents of RMON High-Capacity alarm table.

S6000-ON

Syntax `show rmon hc-alarm [index] [brief]`

Parameters

<i>index</i>	(OPTIONAL) Enter the table index number to display just that entry.
<i>brief</i>	(OPTIONAL) Enter the keyword <code>brief</code> 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
9.7(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.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon hc-alarm 1
RMON high-capacity alarm entry 2
  object: 1.3.6.1.2.1.2.2.1.4.2099844
  sample interval: 10
  sample type: delta value.
  value: 0, value status: positive
  alarm type: rising or falling alarm.
  alarm rising threshold value: positive.
  rising threshold: 500, RMON event index: 3
  alarm falling threshold value: positive.
  falling threshold: 300, RMON event index: 4
  alarm sampling failed 0 times.
  alarm owner:
  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.

S6000-ON

Syntax `show rmon history [index] [brief]`

Parameters

<i>index</i>	(OPTIONAL) Enter the table index number to display just that entry.
<i>brief</i>	(OPTIONAL) Enter the keyword <i>brief</i> 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
9.7(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.
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 2/1/1
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 2/2/1
6002 100974631 TenGigabitEthernet 2/2/1
6003 101236775 TenGigabitEthernet 2/1/1
6004 101236775 TenGigabitEthernet 2/1/1
9001 134529054 TenGigabitEthernet 3/2/1
9002 134529054 TenGigabitEthernet 3/2/1
9003 134791198 TenGigabitEthernet 3/1/1
9004 134791198 TenGigabitEthernet 3/1/1
Dell#
```

show rmon log

Display the contents of the RMON log table.

S6000-ON

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
9.7(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.
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 log br
eventIndex      description
-----
2                2
4                4
Dell#
```

show rmon statistics

Display the contents of RMON Ethernet statistics table.

S6000-ON

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
97(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.
6.1.1.0	Introduced on the E-Series.

Example (Index)

```
Dell#show rmon statistics 6001
RMON statistics entry 6001
  interface: ifIndex.100974631 TenGigabitEthernet 2/1/1
  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 2/2/1
6002       100974631     TenGigabitEthernet 2/2/1
6003       101236775     TenGigabitEthernet 2/1/1
6004       101236775     TenGigabitEthernet 2/1/1
9001       134529054     TenGigabitEthernet 3/2/1
9002       134529054     TenGigabitEthernet 3/2/1
9003       134791198     TenGigabitEthernet 3/1/1
9004       134791198     TenGigabitEthernet 3/1/1
Dell#
```



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.

Dell Networking OS supports RSTP.

bridge-priority

Set the bridge priority for RSTP.

Syntax	<code>bridge-priority priority-value</code> To return to the default value, use the <code>no bridge-priority</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

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.

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 <code>all</code> to debug all spanning tree operations.
bpdu interface {in out}	(OPTIONAL) Enter the keyword <code>bpdu</code> to debug the bridge protocol data units. (OPTIONAL) Enter the keyword <code>interface</code> along with the type slot/port of the interface you want displayed. Type slot/port[/subport] options are the following: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. Optionally, enter an <code>in</code> or <code>out</code> parameter with the optional interface: • For Receive, enter <code>in</code>. • For Transmit, enter <code>out</code>.
events	(OPTIONAL) Enter the keyword <code>events</code> 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
9.7(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.
8.5.1.0	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 gigabitethernet 2/1/1 ?`
 `in Receive (in)`
 `out Transmit (out)`



description

Enter a description of the rapid spanning tree.

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
9.7(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.
pre-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.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
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.

Syntax `forward-delay seconds`
To return to the default setting, use the `no forward-delay` command.

Parameters **seconds** Enter the number of seconds that Dell Networking OS 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
9.7(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.
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).

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 <code>milli-second</code> 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
9.7(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.
8.3.1.0	Added the <code>milli-second</code> 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.

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 Dell Networking OS 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
9.7(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.
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.

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
9.7(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.
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.

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
9.7(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.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(config-rstp)#show config
!
protocol spanning-tree rstp
```



```
no disable
bridge-priority 16384
```

show spanning-tree rstp

Display the RSTP configuration.

Syntax `show spanning-tree rstp [brief] [guard]`

Parameters

brief	(OPTIONAL) Enter the keyword <code>brief</code> to view a synopsis of the RSTP configuration information.
guard	(OPTIONAL) Enter the keyword <code>guard</code> to display the type of guard enabled on an RSTP interface and the current port state.

Command Modes

- EXEC
- EXEC Privilege

Command History	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.
	8.4.2.1	Added support for the optional <code>guard</code> 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).
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
Name      PortID Prio Cost Sts Cost      Designated Bridge ID      PortID
-----
Te 4/2/1 128.418 128 20000 FWD 20000 16384 0001.e801.6aa8 128.418
Te 4/1/1 128.419 128 20000 FWD 20000 16384 0001.e801.6aa8 128.419
Te 4/8/1 128.426 128 20000 FWD 20000 8192 0001.e805.e306 128.130
Te 4/9/1 128.427 128 20000 BLK 20000 8192 0001.e805.e306 128.131

Interface
Name      Role PortID Prio Cost Sts Cost      Link-type Edge
-----
Te 4/2/1 Desg 128.418 128 20000 FWD 20000 P2P      Yes
Te 4/1/1 Desg 128.419 128 20000 FWD 20000 P2P      Yes
Te 4/8/1 Root 128.426 128 20000 FWD 20000 P2P      No
Te 4/9/1 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
Name      PortID Prio Cost Sts Cost      Designated Bridge ID PortID
-----
Te 1/1/1 128.257 128 20000 EDS 0 32768 0001.e801.6aa8 128.257
Interface
Name      Role PortID      Prio Cost Sts Cost Link-type Edge
-----
Te 1/1/1 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 1/1/1
Port 257 (TenGigabitEthernet 1/1/1) 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 1/1/1 0      INCON(Root) Rootguard
Te 1/2/1 0      FWD      Loopguard
Te 1/3/1 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.

Syntax	<code>spanning-tree rstp {cost <i>port-cost</i> edge-port [bpduguard [shutdown-on-violation]] priority <i>priority</i> {loopguard rootguard}}</code>	
Parameters	cost <i>port-cost</i>	Enter the keyword <code>cost</code> then the port cost value. The range is from 1 to 200000. The defaults are: • 100 Mb/s Ethernet interface = 200000 • 1-Gigabit Ethernet interface = 20000 • 10-Gigabit Ethernet interface = 2000 • Port Channel interface with one 100 Mb/s Ethernet = 200000 • Port Channel interface with one 1 Gigabit Ethernet = 20000 • Port Channel interface with one 10 Gigabit Ethernet = 2000 • Port Channel with two 1 Gigabit Ethernet = 18000 • Port Channel with two 10 Gigabit Ethernet = 1800 • Port Channel with two 100 Mbps Ethernet = 180000
	edge-port	Enter the keywords <code>edge-port</code> to configure the interface as a rapid spanning tree edge port.
	bpduguard	(OPTIONAL) Enter the keyword <code>portfast</code> to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the keyword <code>bpduguard</code> to disable the port when it receives a BPDU.
	shutdown-on-violation	(OPTIONAL) Enter the keywords <code>shutdown-on-violation</code> to hardware disable an interface when a BPDU is received and the port is disabled.
	priority <i>priority</i>	Enter keyword <code>priority</code> 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 <code>loopguard</code> to enable loop guard on an RSTP port or port-channel interface.
	rootguard	Enter the keyword <code>rootguard</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.



Version	Description
8.3.11.1	Introduced on the Z9000.
8.4.2.1	Added support for the optional <code>guard</code> 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 <code>hardware shutdown-on-violation</code> 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.

Example

```
Dell(conf)#interface tengigabitethernet 4/1/1
Dell(conf-if-gi-4/0)#spanning-tree rstp edge-port
Dell(conf-if-gi-4/0)#show config
!
interface TenGigabitEthernet 4/1/1
  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.

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
9.7(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.
6.5.1.0	Introduced on the E-Series.

Usage Information By default, Dell Networking OS 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.



Security

The commands in this chapter are available on Dell Networking OS.

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](#)
- [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: Dell Networking OS implements LEAP with MSCHAP v2 supplicant.

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.

Syntax

```
aaa accounting {system | exec | commands level | role role-name} {name |
default}{start-stop | wait-start | stop-only} {tacacs+}
To disable AAA Accounting, use the no aaa accounting {system | exec | command level}
{name | default}{start-stop | wait-start | stop-only} {tacacs+} command.
```

Parameters

system	Enter the keyword <code>system</code> to send accounting information of any other AAA configuration.
exec	Enter the keyword <code>exec</code> to send accounting information when a user has logged in to EXEC mode.



commands {level role role-name}	Enter the keyword <code>command</code> then a privilege level for accounting of commands executed at that privilege level or enter the keyword <code>role</code> then the role name for accounting of commands executed by a user with that user role.
name default	Enter one of the following: - For <code>name</code>, enter a user-defined name of a list of accounting methods. - For <code>default</code>, the default accounting methods used.
start-stop	Enter the keywords <code>start-stop</code> 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 <code>wait-start</code> to ensure that the TACACS+ security server acknowledges the start notice before granting the user’s process request.
stop-only	Enter the keywords <code>stop-only</code> to instruct the TACACS+ security server to send a “stop record accounting” notice at the end of the requested user process.
tacacs+	Enter the keyword <code>tacacs+</code> to use TACACS+ data for accounting. The Dell Networking OS currently only supports TACACS+ 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
9.7(0.0)	Introduced on the S6000–ON.
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.
8.3.19.0	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 In the example above, 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.

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.

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
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
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 Dell Networking OS 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.

Syntax	<code>accounting {exec commands {level role <i>role-name</i>} <i>method-list</i></code>	
Parameters	<i>exec</i>	Enter the keyword <code>exec</code> to apply an EXEC level accounting method list.
	<i>commands {level role <i>role-name</i>}</i>	Enter the keywords <code>commands level</code> to apply an EXEC and CONFIGURATION level accounting method list by enter the keyword <code>role</code> and then the role name for accounting of commands executed by a user with that user role.
	<i>method-list</i>	Enter a method list that you defined using the <code>aaa accounting exec</code> or <code>aaa accounting commands</code> .

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
9.7(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.
7.6.1.0	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 accounting](#) — enables AAA Accounting and creates a record for monitoring the accounting function.

aaa radius group

Configure the RADIUS server group that is used for Authentication, Authorization and Accounting.

Syntax `aaa radius group group-name`
To remove the RADIUS group configuration, use the `no aaa radius group group-name` command.

Parameters ***group-name*** Enter the name of the RADIUS server group.



Defaults	none						
Command Modes	CONFIGURATION						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr> <tr> <td>9.4.(0.0)</td><td>Introduced on the S-Series and Z-Series.</td></tr> </table>	Version	Description	9.7(0.0)	Introduced on the S6000–ON.	9.4.(0.0)	Introduced on the S-Series and Z-Series.
Version	Description						
9.7(0.0)	Introduced on the S6000–ON.						
9.4.(0.0)	Introduced on the S-Series and Z-Series.						
Usage Information	You can use this command to configure the group of Radius servers used for Authentication, Authorization, and Accounting purposes. If the RADIUS group is not configured for Authentication, Authorization, and Accounting, then globally configured Radius servers are used for the purposes. When the RADIUS group is removed, the AAA configuration is also removed.						
Example	<pre> Dell(conf)#radius-server group group1 Dell(conf-radius-group)#radius-server host 1.1.1.1 key secret Dell(conf-radius-group)#radius-server host 2.2.2.2 key secret Dell(conf-radius-group)#radius-server vrf vrfl source-interface tengigabitethernet 1/24/1 Dell(conf)#exit Dell(conf)#aaa radius group group1 </pre>						

show accounting

Display the active accounting sessions for each online user.

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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> </table>	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.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.
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.																
7.6.1.0	Introduced on the S-Series.																
7.5.1.0	Introduced on the C-Series.																



Version	Description
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 admin Priv 1 Role
    Task ID 2, EXEC Accounting record, 00:02:03 Elapsed, service=shell
Active accounted actions on tty3, User ad Priv 15 Role
    Task ID 7, EXEC Accounting record, 00:01:22 Elapsed, service=shell
Active accounted actions on tty4, User ad Priv 15 Role
    Task ID 11, EXEC Accounting record, 00:00:35 Elapsed, service=shell
Active accounted actions on tty5, User ad1 Priv 1 Role sysadmin
    Task ID 16, EXEC Accounting record, 00:00:04 Elapsed, service=shell
Dell#
```

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.

Syntax `authorization {exec | commands {level | role role-name}} method-list`

Parameters

exec	Enter the keyword <code>exec</code> to apply an EXEC level authorization method list.
commands {level role role-name}	Enter the keyword <code>commands</code> followed by either a privilege level for accounting of commands executed at that privilege level, or enter the keyword <code>role</code> 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 <code>aaa accounting exec</code> or <code>aaa accounting commands</code> .

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
9.7(0.0)	Introduced on the S6000–ON.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, and MXL.
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.
7.6.1.0	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.

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 <code>commands</code> then the command privilege level for command level authorization.
	role role-name	Enter the keyword <code>role</code> 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 <code>none</code> 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
9.7(0.0)	Introduced on the S6000–ON.
9.5(0.0)	Added support for roles on the Z9000, S6000, S4820T, S4810, MXL



Version	Description
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	Added support for RADIUS.

aaa authorization config-commands

Set parameters that restrict (or permit) a user's access to EXEC level commands.

Syntax	<pre>aaa authorization config-commands</pre> Disable authorization checking for CONFIGURATION level commands using the <code>no aaa authorization config-commands</code> command.
Defaults	Enabled when you configure <code>aaa authorization commands</code> command.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. 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.
9.0.2.0	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 E-Series.

Usage Information	By default, the <code>aaa authorization commands</code> command configures the system to check both EXEC level and CONFIGURATION level commands. Use the command <code>no aaa authorization config-commands</code> to enable only EXEC-level command checking.

aaa authorization exec

Set parameters that restrict (or permit) a user's access to EXEC-level commands.

Syntax	<pre>aaa authorization exec {name default} {local tacacs+ if- authenticated none}</pre>



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 <code>none</code> 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
9.0.2.0	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	Added support for RADIUS.

privilege level (CONFIGURATION mode)

Change the access or privilege level of one or more commands.

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: • <code>configure</code> for CONFIGURATION mode • <code>exec</code> for EXEC mode • <code>interface</code> for INTERFACE modes • <code>line</code> for LINE mode • <code>route-map</code> for ROUTE-MAP mode • <code>router</code> for ROUTER OSPF, ROUTER RIP, ROUTER ISIS and ROUTER BGP modes



level <i>level</i>	Enter the keyword <code>level</code> 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 <code>reset</code> 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
9.7(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.
pre-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.

Syntax `privilege level level`
To delete access to a terminal line, use the `no privilege level level` command.

Parameters

level <i>level</i>	Enter the keyword <code>level</code> 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 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.
9.0.2.0	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.
pre-6.1.1.0	Introduced on the E-Series.

Obscure Password Commands

To enable the obscure password, use the following commands.

service obscure-passwords

Enable the obscuring of passwords and keys.

Syntax	<code>service obscure-passwords</code> Enable the obscuring of passwords and keys, including RADIUS, TACACS+ keys, router authentication strings, VRRP authentication, use the <code>service obscure-passwords</code> command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.6(0.0)	Introduced on the S4810, S4820T, S5000, S6000, Z9000, Z9500, MXL

Usage Information	By default, the <code>service password-encryption</code> command stores encrypted passwords. For greater security, you can also use the <code>service obscure-passwords</code> 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 <code>service obscure-passwords</code> 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.

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).

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 <code>default</code> then the authentication methods to use as the default sequence of methods for the Enable login. The default is <code>default enable</code> .
<i>method-list-name</i>	Enter a text string (up to 16 characters long) to name the list of enabled authentication methods activated at login.
<i>method</i>	Enter one of the following methods: • <code>enable</code>: use the password the <code>enable password</code> command defines in CONFIGURATION mode. • <code>line</code>: use the password the <code>password</code> command defines in LINE mode. • <code>none</code>: no authentication. • <code>radius</code>: use the RADIUS servers configured with the <code>radius-server host</code> command. • <code>tacacs+</code>: use the TACACS+ server(s) configured with the <code>tacacs-server host</code> command.
<i>... method2</i>	(OPTIONAL) In the event of a “no response” from the first method, Dell Networking OS 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
9.7(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.
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`, Dell Networking OS 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, Dell Networking OS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, Dell Networking OS 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`).

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

<i>method-list-name</i>	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 <code>default</code> to specify that the method list specified is the default method for all terminal lines.



method	Enter one of the following methods: • <code>enable</code>: use the password the <code>enable password</code> command defines in CONFIGURATION mode. Not available if role-only is in use. • <code>line</code>: use the password the <code>password</code> command defines in LINE mode. Not available if role-only is in use. • <code>local</code>: use the password for the userid contained in the local password database. • <code>none</code>: no authentication. Not available if role-only is in use. • <code>radius</code>: use the RADIUS servers configured with the <code>radius-server host</code> command. • <code>tacacs+</code>: use the TACACS+ servers configured with the <code>tacacs-server host</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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(0.0)	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.
pre-6.2.1.0	Introduced on the E-Series.

Usage Information	By default, the locally configured username password is used. If you configure <code>aaa authentication login default</code> , Dell Networking OS 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, Dell Networking OS 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, Dell Networking OS employs the second method (or third method, if necessary) automatically. For example, if the TACACS+ server is reachable, but the server key is invalid, Dell Networking OS 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.

access-class

Restrict incoming connections to a particular IP address in a defined IP access control list (ACL).

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
9.7(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.
pre-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.

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 <i>level</i>	(OPTIONAL) Enter the keyword <code>level</code> then a number as the level of access. The range is from 1 to 15.
<i>encryption-type</i>	(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 <code>show running-config</code> file of another Dell Networking router.
<i>password</i>	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
9.7(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.
pre-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 restricted

Allows Dell Networking technical support to access restricted commands.

Syntax `enable restricted [encryption-type] password`
To disallow access to restricted commands, use the `no enable restricted` command.

Parameters

<i>encryption-type</i>	(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 <code>show running-config</code> file of another Dell Networking router.
<i>password</i>	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
9.7(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.
pre-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.

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 <code>level</code> 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 <code>show running-config</code> 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
9.7(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.
pre-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 configure authentication for console or remote access, apply an authentication method list.

Syntax `login authentication {method-list-name | default}`
To use the local user/password database for login authentication, use the `no login authentication` command.

Parameters

<i>method-list-name</i>	Enter the keywords <code>method-list-name</code> to specify that method list, created in the <code>aaa authentication login</code> command, to be applied to the designated terminal line.
<i>default</i>	Enter the keyword <code>default</code> to specify that the default method list, created in the <code>aaa authentication login</code> 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
97(0.0)	Introduced on the S6000–ON.
9.6.0.0	Revised introductory and usage guidelines 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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.2.1.0	Introduced on the E-Series.

Usage Information When configuring authentication, consider the following:



- If you configure the default authentication list using the `default` keyword, the list applies it to all the local and remote connections globally, unless you have specified some another authentication list for a specific connection.
- If you configure an authentication lists other than default, you must apply those authentication lists to each connection.
- 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.

Syntax `password [encryption-type] password`
 To delete a password, use the `no password password` command.

Parameters

<i>encryption-type</i>	(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.
<i>password</i>	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
9.7(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.
pre-6.1.1.0	Introduced on the E-Series.

Usage Information Dell Networking OS 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 Dell Networking OS .

[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).

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 <i>number</i>	(OPTIONAL) Enter the keywords <code>min-length</code> then the number of characters. The range is from 0 to 32 characters.
max-retry <i>number</i>	(OPTIONAL) Enter the keywords <code>max-retry</code> then the number of maximum password retries. The range is from 0 to 16.
lockout-period <i>minutes</i>	(OPTIONAL) Enter the keyword <code>lockout-period</code> 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 <code>character-restriction</code> to indicate a character restriction for the password.
upper <i>number</i>	(OPTIONAL) Enter the keyword <code>upper</code> then the upper number. The range is from 0 to 31.
lower <i>number</i>	(OPTIONAL) Enter the keyword <code>lower</code> then the lower number. The range is from 0 to 31.
numeric <i>number</i>	(OPTIONAL) Enter the keyword <code>numeric</code> then the numeric number. The range is from 0 to 31.
special-char <i>number</i>	(OPTIONAL) Enter the keywords <code>special-char</code> then the number of special characters permitted. The range is from 0 to 31. The following special characters are supported: ! " # % & ' () ; < = > ? [\] * + , - . / : ^ _ { } ~ @ \$

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
9.7(0.0)	Introduced on the S6000–ON.
9.5(0.0)	Introduced <code>lockout-period</code> 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.

Related Commands [password](#) — specifies a password for users on terminal lines.

service password-encryption

Encrypt all passwords configured in Dell Networking OS.

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
9.7(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.



Version	Description
pre-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.

show privilege

View your access level.

Syntax `show privilege`

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
9.7(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.
pre-6.1.1.0	Introduced on the E-Series.

Example

```
Dell#show privilege
Current privilege level is 15.
Dell#

Dell#show privilege
Current privilege level is 14.
Dell#

Dell#show privilege
Current privilege level is 10.
Dell#
```

Related Commands [privilege level \(CONFIGURATION mode\)](#) — assigns access control to different command modes.



show users

Allows you to view information on all users logged in to the switch.

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
9.7(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.
7.6.1.0	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 The following describes the `show user` 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           Priv
Host(s)  Location
*  0  console 0      unassigned      1  idle
      2  vty 0      admin          unassigned      1
idle      10.16.127.35
      3  vty 1      ad            unassigned      15
idle      10.16.127.145
      4  vty 2      ad1          sysadmin        1
idle      10.16.127.141
      5  vty 3      ad1          sysadmin        1
idle      10.16.127.145
```



```

        6 vty 4          admin          unassigned          1
idle    10.16.127.141
        7 vty 5          ad            unassigned          15
idle    10.16.127.141
Dell#

```

Related Commands [username](#) — enables a user.

timeout login response

Specify how long the software waits for the login input (for example, the user name and password) before timing out.

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
9.7(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.
pre-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} [encryption-type] password] [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

<i>name</i>	Enter a text string for the name of the user up to 63 characters.
<i>access-class</i> <i>access-list-name</i>	Enter the keywords <code>access-class</code> then the name of a configured access control list (either an IP access control list or MAC access control list).
<i>nopassword</i>	Enter the keyword <code>nopassword</code> to specify that the user should not enter a password.
<i>password</i>	Enter the keyword <code>password</code> then the <code>encryption-type</code> or the password.
<i>secret</i>	Enter the keyword <code>secret</code> then the <code>encryption-type</code> or the password.
<i>encryption-type</i>	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 <code>password</code> option. • 7 to indicate that a password encrypted using a DES hashing algorithm follows. This encryption type is available with the <code>password</code> option only. • 5 to indicate that a password encrypted using an MD5 hashing algorithm follows. This encryption type is available with the <code>secret</code> option only, and is the default encryption type for this option.
<i>password</i>	Enter a string up to 32 characters long.
<i>privilege level</i>	Enter the keyword <code>privilege</code> then a number from zero (0) to 15.
<i>role role-name</i>	Enter the keyword <code>role</code> followed by the role name to associate with that user ID.
<i>secret</i>	Enter the keyword <code>secret</code> then the encryption type.

Defaults The default encryption type for `password` option is **0**. The default encryption type for `secret` option is **0**.
The default value of `privilege level` is **1**.

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(0.0)	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.



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	Added support for the <code>secret</code> 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.

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.

debug radius

View RADIUS transactions to assist with troubleshooting.

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
9.7(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.



Version	Description
pre-6.2.1.0	Introduced on the E-Series.

ip radius source-interface

Specify an interface's IP address as the source IP address for RADIUS connections.

Syntax `ip radius source-interface interface`
 To delete a source interface, use the `no ip radius source-interface` command.

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a Null interface, enter the keyword <code>null</code> then the Null interface number. - For a VLAN interface, enter the keyword <code>vlan</code> 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.
9.0.2.0	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.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.2.1.0	Introduced on the E-Series.



radius-server deadtime

Configure a time interval during which non-responsive RADIUS servers to authentication requests are skipped.

Syntax	<code>radius-server deadtime seconds</code> To disable this function or return to the default value, use the <code>no radius-server deadtime</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.
pre-6.1.1.0	Introduced on the E-Series.

radius-server group

Creates or deletes a group of radius servers.

Syntax	<code>radius-server group group-name</code>	
Parameters	group-name	Enter the group name that denotes the group of RADIUS servers.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.



Version	Description
9.4.(0.0)	Introduced on the S-Series and Z-Series.

Example

```
Dell(config)#radius-server group group1
Dell(config-radius-group)#radius-server host 1.1.1.1 key secret
Dell(config-radius-group)#radius-server host 2.2.2.2 key secret
Dell(config-radius-group)#radius-server vrf vrf1 source-interface
tengigabitethernet 1/3/1
Dell(config-radius-group)#show config
!
radius-server group group1
radius-server vrf vrf1 source-interface TenGigabitEthernet 1/3/1
radius-server host 1.1.1.1 key 7 9a2f3ec0c65c6f41
radius-server host 2.2.2.2 key 7 9a2f3ec0c65c6f41
Dell(config-radius-group)#
```

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 host

Configure a RADIUS server host.

Syntax

```
radius-server host {hostname | ipv4-address | ipv6-address} [auth-port
port-number] [retransmit retries] [timeout seconds] [key [encryption-type]
key]
```

Parameters

<i>hostname</i>	Enter the name of the RADIUS server host.
<i>ipv4-address ipv6-address</i>	Enter the IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) of the RADIUS server host.
<i>auth-port port-number</i>	(OPTIONAL) Enter the keywords <i>auth-port</i> then a number as the port number. The range is from zero (0) to 65535. The default port-number is 1812 .
<i>retransmit retries</i>	(OPTIONAL) Enter the keyword <i>retransmit</i> then a number as the number of attempts. This parameter overwrites the <i>radius-server retransmit</i> command. The range is from zero (0) to 100. The default is 3 attempts .
<i>timeout seconds</i>	(OPTIONAL) Enter the keyword <i>timeout</i> then the seconds the time interval the switch waits for a reply from the RADIUS server. This parameter overwrites the <i>radius-server timeout</i> command. The range is from 0 to 1000. The default is 5 seconds .
<i>key [encryption-type] key</i>	(OPTIONAL) Enter the keyword <i>key</i> 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

- RADIUS SERVER GROUP
- 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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.4.1.0	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.
pre-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. Dell Networking OS 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.

You can use duplicate host names or IP addresses among RADIUS groups. However, you cannot use duplicate host names or IP addresses within the same RADIUS group. If a VRF is not configured on the RADIUS group, then servers configured in the group are considered to be on the default VRF. RADIUS servers that are configured in the CONFIGURATION mode are also considered to be on the default VRF.

You must configure the RADIUS group explicitly with the `aaa radius group` command in order for the AAA servers to use the group of RADIUS servers. The 802.1x servers use the group of RADIUS servers based on the VRF where the 802.1x request is received. As a result, it is possible that both globally configured RADIUS servers as well as the group-configured RADIUS servers (without VRF or default VRF) are used for processing the 802.1x requests that are received at the default VRF. The order in which the RADIUS servers are tried depends on the order in which the RADIUS servers are configured.



Example

```
Dell(conf)#radius-server group group1
Dell(conf-radius-group)#radius-server host 1.1.1.1 key secret
Dell(conf-radius-group)#no radius-server host 1.1.1.1
```

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 vrf

Create an association between a RADIUS server group and a VRF and source interface.

ud

Syntax

```
radius-server vrf vrf-name [source-interface interface]
```

To delete the association between a RADIUS server group and a VRF and source interface, use the `no radius-server vrf vrf-name [source-interface interface]` command.

Parameters

vrf vrf-name Enter the keyword `vrf` and then the name of the VRF to associate a RADIUS server group with that 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/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.

Defaults Not configured.

Command Modes RADIUS SERVER 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
9.7(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 You can use this command to associate a group of RADIUS servers with a VRF and source interface. You can configure the source interface only with the VRF attribute and source interface is optional with the VRF attributes.

If VRF is not configured on the RADIUS group, then the group is considered to be on the default VRF. It is possible to use the default VRF name; however, you cannot configure the source interface with the default VRF as such a configuration results in conflicts between the source interfaces corresponding to the 802.1x supplicants on that default VRF.

RADIUS groups and VRFs have one-to-one mapping. If a VRF is configured with one RADIUS group, then you cannot use the same VRF with another RADIUS group. When the VRF is removed, then the corresponding RADIUS group is also removed automatically.

Example

```
Dell(conf)#radius-server group group1
Dell(conf-radius-group)#radius-server vrf vrf1 source-interface
tengigabitethernet 1/30/1

Dell(conf)#radius-server group group2
Dell(conf-radius-group)#radius-server vrf default
```

radius-server key

Configure a key for all RADIUS communications between the switch and the RADIUS host server.

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
9.7(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.



Version	Description
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.
pre-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.

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 FTOS 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
9.7(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.
pre-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 .

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 the Dell Networking OS 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
9.7(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.
pre-6.2.1.0	Introduced on the E-Series.

Related Commands [radius-server host](#) — configures a RADIUS host.

TACACS+ Commands

Dell Networking OS supports TACACS+ as an alternate method for login authentication.

tacacs-server group

Creates a group of TACACS servers to be used for Authentication, Authorization, and Accounting..

Syntax `aaa tacacsgroup group-name`

To delete a group of TACACS servers, use the `no tacacs-server group group-name` command

.



Parameters	group-name Enter the name of the TACACS server group.						
Defaults	Not configured.						
Command Modes	CONFIGURATION						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr> <tr> <td>9.4(0.0)</td><td>Introduced on the S-Series and Z-Series.</td></tr> </tbody> </table>	Version	Description	9.7(0.0)	Introduced on the S6000–ON.	9.4(0.0)	Introduced on the S-Series and Z-Series.
Version	Description						
9.7(0.0)	Introduced on the S6000–ON.						
9.4(0.0)	Introduced on the S-Series and Z-Series.						
Usage Information	If the TACACS group is not configured for Authentication, Authorization, and Accounting, then globally configured TACACS servers are used for the purposes. When the TACACS group is removed, the AAA configuration is also removed.						
Example	<pre>Dell(config)#tacacs-server group group1 Dell(config-tacacs-group)#tacacs-server host 1.1.1.1 key secret Dell(config-tacacs-group)#tacacs-server host 2.2.2.2 key secret Dell(config-tacacs-group)#tacacs-server vrf vrf1 source-interface tengigabitethernet 1/20/1 Dell(config)#exit Dell(config)#aaa tacacsgroup group1</pre>						
Related Commands	aaa authentication login — specifies the login authentication method. tacacs-server key — configures a TACACS+ key for the TACACS server.						

debug tacacs+

To assist with troubleshooting, view TACACS+ transactions.

Syntax	<code>debug tacacs+</code> To disable debugging of TACACS+, use the <code>no debug tacacs+</code> command.										
Defaults	Disabled.										
Command Modes	EXEC Privilege										
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> </tbody> </table>	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.
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.										



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.
pre-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.

Syntax `ip tacacs source-interface interface`
 To delete a source interface, use the `no ip tacacs source-interface` command.

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. - For a Null interface, enter the keyword <code>null</code> then the Null interface number. - For a VLAN interface, enter the keyword <code>vlan</code> 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.
9.0.2.0	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.
8.3.7.0	Introduced on the S4810.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
pre-6.2.1.1	Introduced on the E-Series.



tacacs-server group

Creates a group of TACACS servers.

Syntax	<code>tacacs-server group group-name</code>	
	To delete a group of TACACS servers, use the <code>no tacacs-server group group-name</code> command.	
Parameters	group-name	Enter the name of the TACACS server group.
Defaults	Not configured.	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	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.
9.4.(0.0)	Introduced on the S-Series and Z-Series.

Usage Information You can associate a TACACS server group with a VRF.

Example

```
Dell(conf)#tacacs-server group group1
Dell(conf-tacacs-group)#tacacs-server host 1.1.1.1 key secret
Dell(conf-tacacs-group)#tacacs-server host 2.2.2.2 key secret
Dell(conf-tacacs-group)#tacacs-server vrf vrf1 source-interface
tengigabitethernet 1/30/1
Dell(conf-tacacs-group)#show config
!
tacacs-server group group1
tacacs-server vrf vrf1 source-interface TenGigabitEthernet 1/30/1
tacacs-server host 1.1.1.1 key 7 9a2f3ec0c65c6f41
tacacs-server host 2.2.2.2 key 7 9a2f3ec0c65c6f41
Dell(conf-tacacs-group)#
```

Related Commands [aaa authentication login](#) — specifies the login authentication method.

[tacacs-server key](#) — configures a TACACS+ key for the TACACS server.

tacacs-server host

Specify a TACACS+ host.

Syntax	<code>tacacs-server host {hostname ipv4-address ipv6-address} [port number]</code> <code>[timeout seconds] [key key]</code>	
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) of the TACACS+ server host.
	port number	(OPTIONAL) Enter the keyword <code>port</code> 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 <code>timeout</code> 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 <code>key</code> then a string up to 42 characters long as the authentication key. This authentication key must match the key specified in the <code>tacacs-server key</code> 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
9.7(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.
8.4.1.0	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.
pre-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.

You can use duplicate host names or IP addresses among TACACS groups. However, you cannot use duplicate host names or IP addresses within the same TACACS group.

If a VRF is not configured on the TACACS group, then servers configured in the group are considered to be on the default VRF. TACACS servers that are configured in the CONFIGURATION mode are also considered to be on the default VRF.

For AAA servers to use a group of TACACS servers, you must explicitly configure the group using the `aaa tacacs group group-name` command. The order in which the TACACS servers are tried depends on the order in which they are configured.



Example

```
Dell(conf)#tacacs-server group group1
Dell(conf-tacacs-group)#tacacs-server host 1.1.1.1 key secret
Dell(conf-tacacs-group)#no tacacs-server host 1.1.1.1
```

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.

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
9.7(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.
7.7.1.0	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.
pre-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.



tacacs-server vrf

Create an association between a TACACS server group and a VRF and source interface.

Syntax `tacacs-server vrf vrf-name [source-interface interface]`
To delete the association between a TACACS server group and a VRF and source interface, use the `no tacacs-server vrf vrf-name [source-interface interface]` command.

Parameters

vrf vrf-name	Enter the keyword <code>vrf</code> and then the name of the VRF to associate a TACACS server group with that VRF.
interface	Enter the following keywords and slot/port or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a Null interface, enter the keyword <code>null</code> then the Null interface number. - For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.

Defaults Not configured.

Command Modes TACACS SERVER 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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S-Series and Z-Series.

Usage Information You can use this command to associate a group of TACACS servers with a VRF and source interface. You can configure the source interface only with the VRF attribute and source interface is optional with the VRF attributes.

If VRF is not configured on the TACACS group, then the group is considered to be on the default VRF.

RADIUS groups and VRFs have one-to-one mapping. If a VRF is configured with one RADIUS group, then you cannot use the same VRF with another RADIUS group. When the VRF is removed, then the corresponding RADIUS group is also removed automatically.

Example

```
Dell(conf)#tacacs-server group group1
Dell(conf-tacacs-group)#tacacs-server vrf vrf1 source-interface
tengigabitethernet 1/3/1

Dell(conf)#tacacs-server group group2
```



```
Dell(conf-tacacs-group)#tacacs-server vrf default
```

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.

Dell Networking OS supports RADIUS and Active Directory environments using 802.1X Port Authentication.

Important Points to Remember

Dell Networking OS 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 supported on Dell Networking OS.
- 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; dot1x must be enabled both globally and at the interface level.

Syntax `dot1x authentication`

To disable dot1x on globally, use the `no dot1x authentication` 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
9.7(0.0)	Introduced on the S6000–ON.
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 C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

Related Commands [dot1x authentication \(Interface\)](#) — enables dot1x on an interface.

dot1x authentication (Interface)

Enable dot1x on an interface; dot1x must be enabled both globally and at the interface level.

Syntax	<code>dot1x authentication</code> To disable dot1x on an interface, use the <code>no dot1x authentication</code> command.
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 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.

Syntax	<code>dot1x auth-fail-vlan <i>vlan-id</i> [max-attempts <i>number</i>]</code> To delete the authentication failure VLAN, use the <code>no dot1x auth-fail-vlan <i>vlan-id</i> [max-attempts <i>number</i>]</code> command.				
Parameters	<table> <tr> <td><i>vlan-id</i></td><td>Enter the VLAN Identifier. The range is from 1 to 4094.</td></tr> <tr> <td><i>max-attempts number</i></td><td>(OPTIONAL) Enter the keywords <code>max-attempts</code> then number of attempts desired before authentication fails. The range is from 1 to 5. The default is 3.</td></tr> </table>	<i>vlan-id</i>	Enter the VLAN Identifier. The range is from 1 to 4094.	<i>max-attempts number</i>	(OPTIONAL) Enter the keywords <code>max-attempts</code> then number of attempts desired before authentication fails. The range is from 1 to 5. The default is 3 .
<i>vlan-id</i>	Enter the VLAN Identifier. The range is from 1 to 4094.				
<i>max-attempts number</i>	(OPTIONAL) Enter the keywords <code>max-attempts</code> 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[/subport])
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
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 (<code>dot1x reauthentication</code>).

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.

Syntax	<code>dot1x auth-server radius</code>
Defaults	none
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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
7.6.1.0	Introduced on the C-Series and S-Series.
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.

Syntax `dot1x guest-vlan vlan-id`
 To disable the guest VLAN, use the `no dot1x guest-vlan vlan-id` command.

Parameters

<i>vlan-id</i>	Enter the VLAN Identifier. The range is from 1 to 4094.

Defaults Not configured.

Command Modes CONFIGURATION (conf-if-interface-slot/port[/subport])

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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 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, Dell Networking OS attempts to authenticate the host based on its MAC address.

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
9.7(0.0)	Introduced on the S6000–ON.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.4	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.

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
9.7(0.0)	Introduced on the S6000–ON.
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 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.

Syntax `dot1x port-control {force-authorized | auto | force-unauthorized}`

Parameters

force-authorized	Enter the keywords <code>force-authorized</code> to forcibly authorize a port.
auto	Enter the keyword <code>auto</code> to authorize a port based on the 802.1X operation result.
force-unauthorized	Enter the keywords <code>force-unauthorized</code> 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
9.7(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 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.

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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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 C-Series and S-Series.
7.4.1.0	Introduced on the E-Series.

dot1x reauthentication

Enable periodic re-authentication of the client.

Syntax	<code>dot1x reauthentication [interval seconds]</code> To disable periodic re-authentication, use the <code>no dot1x reauthentication</code> command.

Parameters	interval seconds	(Optional) Enter the keyword <code>interval</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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 C-Series and S-Series.



Version	Description
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.

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
9.7(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 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.

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
9.7(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 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.

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
9.7(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 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.

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 (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
9.7(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 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.

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/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.

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
9.7(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.
8.5.1.0	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 interface fortyGigE 1/10
```

```
802.1x information on Fo 1/10:
```

```
-----
Dot1x Status:           Enable
Port Control:           AUTO
Port Auth Status:       UNAUTHORIZED
Re-Authentication:      Disable
Untagged VLAN id:       None
Guest VLAN:             Disable
Guest VLAN id:          NONE
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:             2
Supplicant Timeout:     30 seconds
Server Timeout:         30 seconds
Re-Auth Interval:       3600 seconds
Max-EAP-Req:            2
Host Mode:              SINGLE_HOST
Auth PAE State:         Initialize
Backend State:          Initialize
Dell#
```

```
Dell# show dot1x interface fortyGigE 1/10
```

```
802.1x information on Fo 1/10:
```

```
-----
Dot1x Status:           Enable
Port Control:           FORCE_AUTHORIZED
Port Auth Status:       UNAUTHORIZED
Re-Authentication:      Disable
Untagged VLAN id:       None
Guest VLAN:             Disable
Guest VLAN id:          NONE
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:                2
Supplicant Timeout:        30 seconds
Server Timeout:            30 seconds
Re-Auth Interval:          3600 seconds
Max-EAP-Req:               2
Host Mode:                 SINGLE_HOST
Auth PAE State:            Initialize
Backend State:             Initialize
Dell#

```

SSH Server and SCP Commands

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 key generate

Generate keys for the SSH server.

Syntax



NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell 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. The default is **1024**.



NOTE: You must have a license to access the FIPS mode. For more information, contact your Dell representative.

rsa1

Enter the keyword `rsa1` then the key size to generate a SSHv1 RSA host keys. The range is from 1024 to 2048.



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 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.
9.0.2.0	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 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.



Version	Description
pre-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), 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(config)#crypto key generate rsa
Enter key size <1024-2048>. Default<1024> :
Host key already exists. Overwrite (y/n)?y
Generating 1024-bit SSHv2 RSA key.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Dell(config)#
Dell(config)#crypto key generate rsa1
Enter key size <1024-2048>. Default<1024> :
Host key already exists. Overwrite (y/n)?y
Generating 1024-bit SSHv1 RSA key.
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Dell(config)#
```

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.

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 <i>Dell Networking OS Command Line Reference Guide</i> .
	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(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL

debug ip ssh

Enables collecting SSH debug information.

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
9.7(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.
pre-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.

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
9.7(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.



Version	Description
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 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.

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
9.7(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.
pre-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 connection-rate-limit

Configure the maximum number of incoming SSH connections per minute.

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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
pre-6.1.1.0	Introduced on the E-Series.

ip ssh hostbased-authentication

Enable hostbased-authentication for the SSHv2 server.

Syntax	<code>ip ssh hostbased-authentication enable</code> To disable hostbased-authentication for SSHv2 server, use the <code>no ip ssh hostbased-authentication enable</code> command.

Parameters	enable Enter the keyword <code>enable</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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
pre-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.

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
9.7(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.
pre-6.1.1.0	Introduced on the E-Series.

Usage Information The server-generated key is used for SSHv1 key-exchange.

ip ssh password-authentication

Enable password authentication for the SSH server.

Syntax	<code>ip ssh password-authentication enable</code> To disable password-authentication, use the <code>no ip ssh password-authentication enable</code> command.																			
Parameters	enable	Enter the keyword <code>enable</code> 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000–ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>pre-6.1.1.0</td><td>Introduced on the E-Series.</td></tr></table>		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.	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.
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.																			
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	With password authentication enabled, you can authenticate using the local, RADIUS, or TACACS+ password fallback order as configured.																			

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.

Syntax	<pre>ip ssh rekey [time rekey-interval] [volume rekey-limit]</pre> To reset to the default, use <code>no ip ssh rekey [time rekey-interval] [volume rekey-limit]</code> command.	
Parameters	time minutes	Enter the keywords <code>time</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL

ip ssh pub-key-file

Specify the file used for host-based authentication.

Syntax	<code>ip ssh pub-key-file {WORD}</code>	
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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.
pre-6.1.1.0	Introduced on the E-Series.

Usage Information	This command specifies the file used for the host-based authentication. The <code>creates/</code> file overwrites the <code>flash://ADMIN_DIR/ssh/knownhosts</code> 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
```



+DWEc3cgYAcU5LailMU2ODrzhCwyDNp05tKBU3t 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 rhostsfile

Specify the rhost file used for host-based authorization.

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
9.7(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.
pre-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.

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
9.7(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.
pre-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).

ip ssh server

Configure an SSH server. SSH server is enabled by default.

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`
- `hmac-sha2-256-96`

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`
- `hmac-sha2-256-96`



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,hmac-sha2-256-96`.
- *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
9.7(0.0)	Introduced on the S6000–ON.
9.5(0.0)	Introduced the <code>cipher</code> , <code>kex</code> and <code>mac</code> options on the Z9000, S6000, S4820T, S4810, and MXL.
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.
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 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.



NOTE: Starting with Dell Networking OS Release 9.2(0.0), SSH server is enabled by default.

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 vrf

Configure an SSH server on either a specific VRF or a management VRF.

Syntax



NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.

```
ip ssh server vrf {management | vrf-name}
```

To disable the SSH server configuration, use the `no ip ssh server vrf {management | vrf-name}` command.

Parameters

vrf management	Enter the key word <code>vrf</code> followed by the keyword <code>management</code> to configure an SSH server on a management VRF.
vrf vrf-name	Enter the key word <code>vrf</code> followed by the VRF name to configure an SSH server on 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
9.7(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 You can enable the SSH server on either a management VRF or a user defined VRF but not both. If no VRF is specified, then the SSH server is enabled on the default VRF.

If the SSH server is enabled on a VRF with name `vrf1`, then use the following command to restart the SSH server on a VRF with name `vrf2`: `ip ssh server vrf vrf2`. If the SSH server is enabled on a VRF with name `vrf1`, then use the following command to restart the SSH server on the default VRF: `ip ssh server vrf`.

Example

- `Dell(conf)#ip ssh server vrf vrf1`
- `Dell(conf)#no ip ssh server vrf`
- `Dell(conf)#ip ssh server vrf management`
- `Dell(conf)#no ip ssh server vrf`

Related Commands [show ip ssh](#) — displays the ssh information.

ip ssh source-interface

Specifies an interface's IP address as the source IP address for an outgoing SSH connections.

Syntax `ip ssh source-interface interface`
To delete a source interface, use the `no ip ssh source-interface` command.

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For a port channel interface, enter the keywords <code>port-channel</code> then a number. The range is from 1 to 128. • For a Null interface, enter the keyword <code>null</code> then the Null interface number. • For a VLAN interface, enter the keyword <code>vlan</code> 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(0.0)	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 1/30/1
Dell(conf)#do ssh 10.10.10.2 -l admin
Dell(conf)#no ip ssh source-interface
```

ip ssh vrf

Specify a VRF for an outgoing SSH connections.

Syntax `ip ssh vrf vrf-name`

To delete a VRF for an outgoing SSH connection, use the `no ip ssh vrf vrf-name` command.

Parameters

vrf vrf-name	Enter the keyword <code>vrf</code> and then the name of the VRF to configure that VRF for an outgoing SSH session.

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(0.0)	Introduced on the Z9500.
9.4(0.0)	Introduced on the S-Series and Z9000.

Usage Information If you configure a VRF for an SSH session, then you need not explicitly mention the same VRF for the SSH client sessions intended for that VRF. The `vrf` attribute in the `ip ssh vrf` command is applicable for both the SSH client as well as the `COPY (SCP)` commands.

Example

```
Dell(conf)#ip ssh vrf vrf1
Dell(conf)#do ssh 10.10.10.2 -l admin
Dell(conf)#no ip ssh vrf vrf1
```

show crypto

Display the public part of the SSH host-keys.

Syntax



NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell representative.

```
show crypto key mypubkey {rsa | rsal}
```

Parameters

Key	Enter the keyword <code>key</code> to display the host public key.
mypubkey	Enter the keyword <code>mypubkey</code> 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, refer to the relevant *Dell Networking OS*.

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.
9.0.2.0	Introduced on the S6000.
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.
pre-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

Example

```
Dell#show crypto key mypubkey rsa1
1024 65537
150477578329696762034442036788963493870885070479991994815292070626705966514872389873

Dell#show crypto key mypubkey rsa
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQGC9IYgcUcc8wQm+5KUQgW/zAs8V5STa1Gq4/+S+6H9axpQn

Dell#
```

Related Commands [crypto key generate](#) — generates the SSH keys.

show ip ssh

Display information about established SSH sessions.

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
9.7(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.
pre-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   : 3des-cbc,aes128-cbc,aes192-cbc,aes256-
cbc,aes128-ctr,aes192-ctr,aes256-ctr.
SSH server macs      : hmac-md5,hmac-md5-96,hmac-sha1,hmac-
sha1-96,hmac-sha2-256,hmac-sha2-256-96.
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
  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.

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
9.7(0.0)	Introduced on the S6000–ON.
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.
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 This command displays the contents of the `flash://ADMIN_DIRssh/knownhosts` file.

Example

```
Dell# show ip ssh client-pub-keys
4.8.1.2 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAu5NoTbmnLxBknaeXZmUJMupNwNUoGlo1/
yLPI5eehQTyalDRPhtGyPlcmMbCH
+QJkqtiwDPmH4njyDMYDCXY85vc55ibWsN9qalagklnh2cj2q4nYj5x8+800hYeFPaHiygd8U/
FXict6ljWs84Co1UTsAgRzDJ9aUSS75TVac= root@dt-maa-linux-1.forcel0networks.c
om
2200:2200:2200:2200:2200::2202 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAu5NoTbmnLxBknaeXZmUJMupNwNUoGlo1/
yLPI5eehQTyalDRPhtGyPlcmMbCH
+QJkqtiwDPmH4njyDMYDCXY85vc55ibWsN9qalagklnh2cj2q4nYj5x8+800hYeFPaHiygd8U/
FXict6ljWs84Co1UTsAgRzDJ9aUSS75TVac= root@dt-maa-li
nux-1.forcel0networks.com
10.16.151.48 ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAu5NoTbmnLxBknaeXZmUJMupNwNUoGlo1/
yLPI5eehQTyalDRPhtGyPlcmMbCH
+QJkqtiwDPmH4njyDMYDCXY85vc55ibWsN9qalagklnh2cj2q4nYj5x8+800hYeFPaHiygd8U/
FXict6ljWs84Co1UTsAgRzDJ9aUSS75TVac=
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.

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, refer to the relevant *Dell 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.
9.0.2.0	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
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 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
AAAAB3NzaC1yc2EAAAABIwAAAIEAyB17l4gFp4r2DRHIvMc1VZd0Sg5GQxRV1y1X1JOMeO6Nd0WuYyzrQMM
4qJAoBwtneOXfLBcHF3V2hcMIqaZN+CRcnw/
zCMlnCf0+qVTdl0ofsea5r09kS0xTp0CNfHXZ3NuGCq9Ov33m9+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.

Syntax

 **NOTE: Some of the parameters in this command require licensing to access. For more information, contact your Dell Networking representative.**

```
ssh {hostname | ipv4 address | ipv6 address} [-c encryption cipher | -l
username | -m HMAC algorithm | -p port-number | -v {1 | 2}]
```

Parameters

hostname	(OPTIONAL) Enter the IP address or the host name of the remote device.
vrf instance	(OPTIONAL) E-Series Only: Enter the keyword <code>vrf</code> 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`: 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



-l <i>username</i>	(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 <i>HMAC algorithm</i>	Enter one of the following HMAC algorithms to use. (For v2 clients only): "no fips mode enable"(disable) will support v1 & v2 client. • 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. • hmac-sha2-256-96: Force ssh to use hmac-sha2-256-96 HMAC algorithm.
-p <i>port-number</i>	(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
9.7(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.
8.3.12.0	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.
pre-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 10.16.151.48 -l anvltest

Trying 10.16.151.48...
01:18:16: %STKUNIT0-M:CP %SEC-5-SSH_USAGE: Initiated SSH Client v2 (FIPS
Disabled) to anvltest@10.16.151.48 by default from console
anvltest@10.16.151.48's password:
Last login: Thu Jan  5 00:17:47 2012 from login-maa-101
```



```
[anvltest@dt-maa-linux-1 ~]# exit
logout
Dell#
```

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.

Syntax	<code>clear ip dhcp snooping binding</code>
Defaults	none
Command Modes	EXEC Privilege
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

Related Commands [show ip dhcp snooping](#) — displays the contents of the DHCP binding table.

ip dhcp relay

Enable Option 82.

Syntax	<code>ip dhcp relay information-option [trust-downstream</code>		
Parameters	<table><tr><td>trust-downstream</td><td>Configure the system to trust Option 82 when it is received from the previous-hop router.</td></tr></table>	trust-downstream	Configure the system to trust Option 82 when it is received from the previous-hop router.
trust-downstream	Configure the system to trust Option 82 when it is received from the previous-hop router.		
Defaults	Disabled.		
Command Modes	CONFIGURATION		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .		

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



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.

ip dhcp snooping

Enable DHCP Snooping globally.

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
9.7(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 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.

Syntax [no] ip dhcp snooping binding mac *address* *vlan-id* *vlan-id* ip *ip-address*
interface *type slot/port* lease *number*

Parameters

mac <i>address</i>	Enter the keyword <i>mac</i> then the MAC address of the host to which the server is leasing the IP address.
vlan-id <i>vlan-id</i>	Enter the keywords <i>vlan-id</i> then the VLAN to which the host belongs. The range is from 2 to 4094.
ip <i>ip-address</i>	Enter the keyword <i>ip</i> then the IP address that the server is leasing.

interface type	Enter the keyword <code>interface</code> then the type of interface to which the host is connected. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383.
slot/port	Enter the slot and port number of the interface.
lease time	Enter the keyword <code>lease</code> 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
9.7(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.
8.5.1.0	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 renew

Renew the binding table.

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
9.7(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 C-Series and S-Series.

ip dhcp snooping trust

Configure an interface as trusted.

Syntax	<code>[no] ip dhcp snooping trust</code>
Defaults	Untrusted
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.

ip dhcp source-address-validation

Enable IP source guard.

Syntax	<code>[no] ip dhcp source-address-validation</code>
Defaults	Disabled.
Command Modes	INTERFACE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.



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	Introduced on the C-Series and S-Series.

ip dhcp snooping vlan

Enable DHCP Snooping on one or more VLANs.

Syntax `[no] ip dhcp snooping vlan name`

Parameters

<i>name</i>	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
9.7(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 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.

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
9.7(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 C-Series and S-Series.

Related Commands [clear ip dhcp snooping](#) — clears the contents of the DHCP binding table.

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.

Syntax `aaa authorization role-only`
To return to the default setting, use the `no aaa authentication role-only` command.

Parameters

<i>name</i>	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).
<i>inherit existing-role-name</i>	Enter the <code>inherit</code> keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).

Defaults none

Command Modes CONFIGURATION



Command History	Version	
	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	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 <code>aaa authorization role-only</code> 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.	
Related Commands	login authentication, password, radius-server host, tacacs-server host	

role

Changes command permissions for roles.

Syntax	<code>role mode { { { addrole deleterole } <i>role-name</i> } reset } command</code>
	To delete access to a command, use the <code>no role mode <i>role-name</i></code>

Parameters	<i>mode</i>	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
	<i>addrole</i>	Enter the keyword <code>addrole</code> to add permission to the command. You cannot add or delete rights for the sysadmin role.
	<i>deleterole</i>	Enter the keyword <code>deleterole</code> to remove access to the command. You cannot add or delete rights for the sysadmin role.
	<i>role-name</i>	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 <code>reset</code> 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
	9.7(0.0)	Introduced on the S6000-ON.
	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, and MXL.
Related Commands	userrole	

show role

Display information on permissions assigned to a command, including user role and/or permission level.

Syntax `show role mode {mode} {command}`

Parameters	<i>command</i>	Enter the command's keywords to assign the command to a certain access level. You can enter one or all of the keywords.
	<i>mode mode</i>	Enter keyword then one of the following modes. • <code>configure</code> • <code>exec</code> • <code>interface</code> • <code>line</code> • <code>route-map</code> • <code>router</code>

Defaults	none							
Command Modes	EXEC Privilege							
Command History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.5(0.0)</td><td>Introduced on the Z9000, S6000, S4820T, S4810, MXL</td></tr></table>		Version	Description	9.7(0.0)	Introduced on the S6000-ON.	9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL
Version	Description							
9.7(0.0)	Introduced on the S6000-ON.							
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
```

Related Commands [userrole](#), `username`, `privilege`

show userroles

Display information on all defined user roles.

Syntax `show userroles`

Example

```
Dell#show userroles
Role           Inheritance  Modes
netoperator
netadmin       Exec
               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
```

Command Modes EXEC Privilege

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.0)	Introduced on the Z9000, S6000, S4820T, S4810, MXL.

Related Commands [userrole](#), `username`

userrole

Create user roles for the role-based security model.

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	<i>name</i>	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).
	<i>inherit existing-role-name</i>	Enter the <code>inherit</code> keyword then specify the system defined role to inherit permissions from (sysadmin, secadmin, netadmin, netoperator).

Defaults none

Command Modes CONFIGURATION

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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.

Related Commands

role mode { { { **addrole** | **deleterole** } *role-name* } | **reset** } *command* – Modifies (adds or deletes) command permissions for newly created user roles and system defined roles.

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.

Dell Networking OS supports L2PT on Dell Networking OS.

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.

debug protocol-tunnel

Enable debugging to ensure incoming packets are received and rewritten to a new MAC address.

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 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. The range is from 1 to 128.

in out both	Enter the keyword <code>in</code> , <code>out</code> , or <code>both</code> to debug incoming interfaces, outgoing interfaces, or both incoming and outgoing interfaces.
vlan <i>vlan-id</i>	Enter the keyword <code>vlan</code> then the VLAN ID. The range is from 1 to 4094.
count <i>value</i>	Enter the keyword <code>count</code> 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
9.7(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.
8.5.1.0	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.

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 <i>rate</i>	Enter the keyword <code>rate-limit</code> 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 <code>stp</code> 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, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
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 1/2/1-3
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.

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
9.7(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.



Version	Description
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.

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
9.7(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.
7.4.1.0	Introduced

Usage Information Dell Networking OS must have the default CAM profile with the default microcode before you enable L2PT.

protocol-tunnel rate-limit

Enable traffic rate limiting per box.

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 75 to 3000. The default is 75 .

Defaults **75** frames per second.

Command Modes CONF-IF-VLAN-STACK



Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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, 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-if-vl-2)#vlan-stack compatible
Dell(conf-if-vl-2-stack)#protocol-tunnel rate-limit 100 <<<<<<< VLAN
stack mode
Dell(conf-if-vl-2-stack)#show config
!
interface Vlan 2
 no ip address
 mtu 1000
 vlan-stack compatible
 protocol-tunnel rate-limit 100
 shutdown
```

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.

Syntax `show protocol-tunnel [vlan vlan-id]`

Parameters

vlan <i>vlan-id</i>	(OPTIONAL) Enter the keyword <code>vlan</code> 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
9.7(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, E-Series and E-Series ExaScale.
7.4.1.0	Introduced

Example

```
Dell#show protocol-tunnel
System Rate-Limit: 75 frames/second
VLAN  Protocols  Interface
1000  STP,PVST     Te 5/7,Te 5/6
1001  LLDP,GVRP    Te 5/7,Te 5/6
1002  MMRP,MVRP    Te 5/7,Te 5/6
1003  LACP,DOT1X   Te 5/7,Te 5/6
1004  OAM,PAUSE    Te 5/7,Te 5/6
1005  E-LMI        Te 5/7,Te 5/6
```

```
Dell#show protocol-tunnel
System Rate-Limit: 75 frames/second
VLAN  Protocols  Interface
1000  STP,PVST     Te 5/7/1,Te 5/6/1
1001  LLDP,GVRP    Te 5/7/1,Te 5/6/1
1002  MMRP,MVRP    Te 5/7/1,Te 5/6/1
1003  LACP,DOT1X   Te 5/7/1,Te 5/6/1
1004  OAM,PAUSE    Te 5/7/1,Te 5/6/1
1005  E-LMI        Te 5/7/1,Te 5/6/1
```

Example (Specific VLAN)

```
Dell#show protocol-tunnel vlan 2
System Rate-Limit: 1000 Frames/second
Interface  Vlan  Protocol(s)
Te1/2/1/1  2      STP, PVST
Dell#
```

Related Commands [show running-config](#) — displays the current configuration.



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](#)).

sflow collector

Configure a collector device to which sFlow datagrams are forwarded.

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 <code>agent-addr</code> 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 <code>max-datagram-size</code> then the size number in bytes. The range is from 400 to 1500. The default is 1400 .
vrf management	(OPTIONAL) Enter the keyword <code>vrf</code> followed by the keyword <code>management</code> to configure the collector device corresponding to the default VRF and the management VRF respectively.

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.
9.4.(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 <code>no</code> form of the command to mirror the syntax used to configure.

Version	Description
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: <code>%Error: Different agent-addr attempted for an existing collector.</code>

Example	<code>Dell(config)#sflow collector 10.1.1.25 agent-addr 10.1.1.10 vrf management</code>

sflow enable (Global)

Enable sFlow globally.

Syntax	<code>sflow enable</code> To disable sFlow, use the <code>no sflow enable</code> command.
Defaults	Disabled.
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.



Version	Description
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.

Related Commands [sflow enable \(Interface\)](#) — enables sFlow on interfaces.

sflow ingress-enable

Enable sFlow ingress on interfaces.

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
9.7(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.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.

Related Commands [show sflow](#) — displays the sFlow configuration.

sflow max-header-size extended

Set the maximum header size of a packet to 256 bytes.

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
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
9.7(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.

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

Command History This guide is platform-specific. For command information about other platforms, refer to the relevant *Dell 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.
9.0.2.0	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.

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.)

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
9.7(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 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.

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																						
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>8.3.7.0</td><td>Introduced on the S4810.</td></tr> <tr> <td>8.2.1.0</td><td>Introduced on S-Series Stacking.</td></tr> <tr> <td>8.1.1.0</td><td>Introduced on the E-Series ExaScale.</td></tr> <tr> <td>7.7.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>7.4.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	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.
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.																						
Related Commands	sflow sample-rate (Interface) — changes the interface sampling rate.																						

sflow sample-rate (Interface)

Change the interface default sampling rate.

Syntax	<pre>sflow sample-rate value</pre> To return to the default sampling rate, use the <code>no sflow sample-rate</code> 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 <i>Dell Networking OS Command Line Reference Guide</i>.	



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.
9.0.2.0	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 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

<i>interface</i>	(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/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 the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 1 to 6. The port range is 1.
- For a port channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- For a 100/1000 Ethernet interface, enter the keyword `GigabitEthernet` 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
9.7(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

```
Dell#show sflow
sFlow services are enabled
Egress Management Interface sFlow services are disabled
Global default sampling rate: 32768
Global default counter polling interval: 20
Global default extended maximum header size: 128 bytes
Global extended information enabled: none
1 collectors configured
Collector IP addr: 100.1.1.1, Agent IP addr: 1.1.1.2, UDP port: 6343 VRF:
Default
0 UDP packets exported
0 UDP packets dropped
0 sFlow samples collected

stack-unit 1 Port set 1
  Gi 1/1/1: configured rate 16384, actual rate 16384   <<< sampling rate
based on line speed if global sampling rate is default
Dell#
```



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. Both features are supported on Dell Networking OS.

The chapter contains the following sections:

- [SNMP Commands](#)
- [Syslog Commands](#)

SNMP Commands

The following SNMP commands are available in the Dell Networking OS.

The simple network management protocol (SNMP) is used to communicate management information between the network management stations and the agents in the network elements. Dell Networking OS supports SNMP versions 1, 2c, and 3, supporting both read-only and read-write modes. Dell Networking OS sends SNMP traps, which are messages informing an SNMP management system about the network. Dell Networking OS 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.

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
9.7(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 legacy
command**

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.

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
9.7(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.

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.

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
9.7(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 legacy
command**

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: vlv2creadg      security model: v1
readview : vlv2cdefault    writeview: no write view specified
notifyview: vlv2cdefault   context: no context specified
row status: active
Dell#
```

Related Commands [snmp-server group](#) — configures an SNMP server group.

show snmp user

Display the information configured on each SNMP user name.

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
9.7(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 legacy
command**

Example

```
Dell#show snmp user
User name: vlv2creadu
Engine ID: 0000178B02000001E80214A8
storage-type: nonvolatile      active
Authentication Protocol: None
Privacy Protocol: None
Dell#
```

snmp ifmib ifalias long

Display the entire description string through the Interface MIB, which would be truncated otherwise to 63 characters.

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
9.7(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.
unknown	Introduced on the E-Series.

Example

```
Dell#config!-----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 Dell Networkingswitch: -----!
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:
Dell#config
```

snmp-server community

Configure a new community string access for SNMPv1 v2 and v3.

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

<i>community-name</i>	Enter a text string (up to 20 characters long) to act as a password for SNMP.
ro	Enter the keyword <code>ro</code> to specify read-only permission.
rw	Enter the keyword <code>rw</code> to specify read-write permission.



ipv6 access-list-name	(Optional) Enter the keyword <code>ipv6</code> then an IPv6 ACL name (a string up to 16 characters long).
security-name name	(Optional) Enter the keywords <code>security-name</code> 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
9.7(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.
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 guest 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 contact

Configure contact information for troubleshooting this SNMP node.

Syntax

```
snmp-server contact text
```

To delete the SNMP server contact information, use the `no snmp-server contact` command.

Parameters

<i>text</i>	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
9.7(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 legacy command	



snmp-server enable traps

Enable SNMP traps.

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` — Notification of changes in the BGP process.
- `config` — Notification of changes to the startup or running configuration.
- `ecfm` — Notification of changes to ECFM.
- `ecmp` — Enable an ECMP trap to notify of ECMP or link bundle traffic imbalances.
- `envmon` — For Dell Networking device notifications when an environmental threshold is exceeded.
- `isis` — Notification of intermediate service traps.
- `lACP` — Notification of changes.
- `snmp` — Notification of RFC 1157 traps.
- `stp` — Notification of a state change in the spanning tree protocol (RFC 1493).
- `vlt` — Notification of virtual link trunking.
- `vrrp` — Notification of a state change in a VRRP group.
- `xstp` — 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`
- `syslog-reachable`
- `syslog-unreachable`

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
9.8(0.0)	Added the following two SNMP notification options: <code>syslog-reachable</code> and <code>syslog-unreachable</code> .
9.7(0.0)	Introduced on the S6000-ON.
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.
9.1(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.
E-Series legacy command	

Usage Information Dell Networking OS supports up to 16 SNMP trap receivers.

If you do not configure this command, traps that controlled by this command are not 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 engineID

Configure the name for both the local and remote SNMP engines on the router.

Syntax `snmp-server engineID [local engineID] [remote ip-address udp-port port-number engineID]`

To return to the default, use the `no snmp-server engineID [local engineID] [remote ip-address udp-port port-number engineID]` command.

Parameters

local engineID	Enter the keyword <code>local</code> 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 <code>remote</code> followed by the IP address that identifies the copy of the SNMP on the remote device.



udp-port port-number engineID Enter the keywords `udp-port` followed by the user datagram protocol (UDP) 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
9.7(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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.

E-Series legacy command

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.

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): • <code>v1v2creadg</code> — maps to a community/security-name with <code>ro</code> permissions. • <code>v1v2cwriteg</code> — maps to a community/security-name <code>rw</code> 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 <code>auth</code> to specify authentication of a packet without encryption.
noauth	(OPTIONAL) Enter the keyword <code>noauth</code> to specify no authentication of a packet.
priv	(OPTIONAL) Enter the keyword <code>priv</code> to specify both authentication and then scrambling of the packet.
read name	(OPTIONAL) Enter the keyword <code>read</code> 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 <code>write</code> then a name (a string of up to 20 characters long) as the write view name.
notify name	(OPTIONAL) Enter the keyword <code>notify</code> 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 <code>ipv6</code> 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
9.7(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.
8.3.10.2	Added support for the <code>access</code> 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.

E-Series legacy
command

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.

Syntax

```
snmp-server host ip-address | ipv6-address 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 traps | informs [version 1 | 2c | 3] [auth | noauth | priv] [community-string] [udp-port number] [notification-type]` command.

Parameters

<i>ip-address</i>	Enter the keyword <code>host</code> then the IP address of the host (configurable hosts is limited to 16).
<i>ipv6-address</i>	Enter the keyword <code>host</code> then the IPv6 address of the host in the <code>x::x::x::x</code> format.  NOTE: The <code>::</code> notation specifies successive hexadecimal fields of zero.
<i>traps</i>	(OPTIONAL) Enter the keyword <code>traps</code> to send trap notifications to the specified host. The default is traps .
<i>informs</i>	(OPTIONAL) Enter the keyword <code>informs</code> 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 OS 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` — Enable BGP state change traps.
- `ecfm` — Enable ECFM state change traps.
- `entity` — Enable entity change traps.
- `envmon` — Enable SNMP environmental monitor traps.
- `eoam` — Enable EOAM state change traps
- `ets` — Enable ets traps
- `fips` — Enable FIP Snooping state change traps
- `lACP` — Enable LACP state change traps.
- `isis` — Enable ISIS adjacency change traps
- `pfc` — Enable pfc traps
- `snmp` — Enable SNMP trap
- `stp` — Enable 802.1d state change traps
- `vlt` — Enable VLT traps
- `vrrp` — Enable VRRP state change traps
- `xstp` — Enable 802.1s, 802.1w, and PVST+ state change traps

The default is all trap types are sent to 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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Added support for VRF.
9.0.2.0	Introduced on the S6000.
9.1(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.
E-Series legacy command	

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.

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
9.7(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 legacy command	

snmp-server packetsize

Set the largest SNMP packet size permitted. When the SNMP server is receiving a request or generating a reply, use the `snmp-server packetsize global configuration` command.

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
9.7(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 legacy
command

snmp-server trap-source

Configure a specific interface as the source for SNMP traffic.

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 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.

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
9.7(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.
8.5.1.0	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.
E-Series legacy command	

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.

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): • <code>v1v2creadu</code> — maps to a community with <code>ro</code> permissions. • <code>1v2cwriteu</code> — maps to a community <code>rw</code> permissions.
remote ip-address	Enter the keywords <code>udp-port</code> 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 <code>udp-port</code> 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 <code>encrypted</code> to specify the password appear in encrypted format (a series of digits, masking the true characters of the string).
auth	(OPTIONAL) Enter the keyword <code>auth</code> to specify authentication of a packet without encryption.
md5 sha	(OPTIONAL) Enter the keyword <code>md5</code> or <code>sha</code> to designate the authentication level. • <code>md5</code> — Message Digest Algorithm • <code>sha</code> — 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 <code>priv</code> to initiate a privacy authentication level setting.
des56 aes128	(OPTIONAL) Enter the keyword <code>des56</code> or <code>aes128</code> to specify the encryption mode. • <code>aes128</code> — Use 128 bit AES algorithm in CFB mode for encryption. • <code>des56</code> — 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 <code>ipv6</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.



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.

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 user (for AES128-CFB Encryption)

Specify that AES128-CFB encryption algorithm needs to be used for transmission of SNMP information. The Advanced Encryption Standard (AES) Cipher Feedback (CFB) 128-bit encryption algorithm is in compliance with RFC 3826. RFCs for SNMPv3 define two authentication hash algorithms, namely, HMAC-MD5-96 and HMAC-SHA1-96. These are the full forms or editions of the truncated versions, namely, HMAC-MD5 and HMAC-SHA1 authentication algorithms.

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-cfb} 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-cfb} priv-password] [access
access-list-name | ipv6 access-list-name | access-list-name ipv6 access-
list-name] command.
```

Parameters

<i>auth-password</i>	(OPTIONAL) Enter a text string (up to 20 characters long) password that enables the agent to receive packets from the host and to send packets to the host. Minimum: eight characters long.
<i>aes128</i>	(OPTIONAL) Enter the keyword aes128 to initiate the AES128-CFB encryption algorithm for transmission of SNMP packets.
<i>priv-password</i>	(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 and to decrypt the contents of the message it receives from the agent. Minimum: eight characters long.

Defaults

If no authentication or privacy option is configured, then the messages are exchanged (attempted anyway) without any authentication or encryption.

Command Modes

CONFIGURATION

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.3(0.0)	Added support for the AES128-CFB encryption algorithm on the S4820T, S4810, S6000 and Z-Series platforms

Usage Information

To enable robust, effective protection and security for SNMP packets transferred between the server and the client, you can use the **snmp-server user username group groupname 3 auth authentication-type auth-password priv aes128 priv-password** to specify that AES128-CFB encryption algorithm needs to be used.

You cannot modify the FIPS mode if SNMPv3 users are already configured and present in the system. An error message is displayed if you attempt to change the FIPS mode by using the **fips mode enable** command in Global Configuration mode. You can enable or disable FIPS mode only if SNMPv3 users are not previously set up. Otherwise, you must remove the previously configured users before you change the FIPS mode.

Example

```
Dell# snmp-server user privuser v3group v3 encrypted auth md5
9fc53d9d908118b2804fe80e3ba8763d priv aes128
d0452401a8c3ce42804fe80e3ba8763d
```

Related Commands [show snmp user](#) — Displays the information configured on each SNMP user name.

snmp-server view

Configure an SNMPv3 view.

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

<i>view-name</i>	Enter the name of the view (not to exceed 20 characters).
<i>oid-tree</i>	Enter the OID sub tree for the view (not to exceed 20 characters).



included	(OPTIONAL) Enter the keyword <code>included</code> to include the MIB family in the view.
excluded	(OPTIONAL) Enter the keyword <code>excluded</code> 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
97(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 legacy command	

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.

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 <code>vrf</code> and then the name of the VRF to associate an SNMP agent with that VRF.

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
9.7(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.

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
9.7(0.0)	Introduced on the S6000-ON.
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 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.

Syntax `clear logging`

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
9.7(0.0)	Introduced on the S6000-ON.
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	

Related Commands [show logging](#) — displays logging settings and system messages in the internal buffer.

clear logging auditlog

Clears audit log.

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
9.7(0.0)	Introduced on the S6000-ON.
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.

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
9.7(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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Related Commands [logging buffered](#) — sets the logging buffered parameters.

default logging console

Return the default settings for messages logged to the console.

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
9.7(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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

Related Commands [logging console](#) — sets the logging console parameters.

default logging monitor

Return to the default settings for messages logged to the terminal.

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
9.7(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 legacy command	

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.

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
9.7(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 legacy command	

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.

Syntax `logging {ip-address | ipv6-address | hostname} [{udp {port}} | {tcp {port}}]`
To disable logging, use the `no logging` command.

Parameters

<i>ip-address</i>	Enter the IPv4 address in dotted decimal format.
<i>ipv6-address</i>	Enter the IPv6 address in the x:x:x:x::X format.  NOTE: The :: notation specifies successive hexadecimal fields of zeros.
<i>hostname</i>	Enter the name of a host already configured and recognized by the switch.
<i>udp</i>	Enter the keyword <code>udp</code> to enable transmission of log message over UDP followed by port number. The default port is 514
<i>tcp</i>	Enter the keyword <code>tcp</code> 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
9.7(0.0)	Introduced on the S6000-ON.

Version	Description
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.
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.
8.4.1.0	Added support for IPv6.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

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.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
E-Series legacy command	

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.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.



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.
7.6.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

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 extended

Logs security and audit events to a system log server.

Syntax	<code>logging extended</code>
Defaults	none
Command Modes	CONFIGURATION
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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(0.0)	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 [show logging auditlog](#) — displays audit log, [clear logging auditlog](#) — clears audit log

logging facility

Configure the Syslog facility used for error messages sent to Syslog servers.

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)
- `daemon` (system daemons)
- `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
9.7(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 legacy command	

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).

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
9.7(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.



Version	Description

E-Series legacy
command

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 Dell Networking logging history table.

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
9.7(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 legacy
command

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.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
E-Series legacy command	

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.

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
9.7(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 legacy command	

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.

Syntax `logging source-interface interface`

To disable this command and return to the default setting, use the `no logging source-interface` command.

Parameters

<i>interface</i>	Enter the following keywords and slot/port or number 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 the Management interface on the stack-unit, enter the keyword `ManagementEthernet` then the slot/port information. The slot range is from 1 to 6. The port range is 1.
- For a port channel interface, enter the keywords `port-channel` then a number. The range is from 1 to 128.
- 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.

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.
9.2(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.
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.
E-Series legacy command	

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 Dell Networking OS output.

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 <code>all</code> to ensure that all levels are printed asynchronously.
	level level	Enter the keyword <code>level</code> 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 <code>all</code> 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
9.7(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 legacy command

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.

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
9.7(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, S55.
7.5.1.0	Introduced on the C-Series.
E-Series legacy command	

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.

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
9.7(0.0)	Introduced on the S6000-ON.
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 auditlog

Displays an audit log.

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
9.7(0.0)	Introduced on the S6000-ON.
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

Display the logging settings and system messages logged to the internal buffer of the switch.

Syntax `show logging [number | history [reverse][number] | reverse [number] | summary]`

Parameters

number	(OPTIONAL) Enter the number of messages displayed in the output. The range is from 1 to 65535.
history	(OPTIONAL) Enter the keyword <code>history</code> to view only information in the Syslog history table.
reverse	(OPTIONAL) Enter the keyword <code>reverse</code> to view the Syslog messages in FIFO (first in, first out) order.
summary	(OPTIONAL) Enter the keyword <code>summary</code> 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, refer to the relevant *Dell 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.
9.2(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.
E-Series legacy command	

Example (Partial)

```
Dell#show logging
Syslog logging: enabled
  Console logging: level debugging
  Monitor logging: level debugging
  Buffer logging: level debugging, 5604 Messages Logged, Size (524288
bytes)
  Trap logging: level informational
Oct 8 09:25:37: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor
223.80.255.254 closed. Hold time
expired
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.200.13.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.13 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.14.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.14 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.11.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.5 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.4.1.3 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.4 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.6 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.12 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.15 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.1.1.3 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.200.12.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 1.1.10.2 Up
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Session closed by neighbor
1.1.10.2 (Hold time expired)
Oct 8 09:25:38: %RPM1:RP1 %BGP-5-ADJCHANGE: Neighbor 192.200.14.7 Up
Oct 8 09:26:25: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor
1.1.11.2 closed. Neighbor recycled
Oct 8 09:26:25: %RPM1:RP1 %BGP-5-ADJCHANGE: Connection with neighbor
1.1.14.2 closed. Neighbor recycled
--More--
```

Example (History)

```
Dell#show logging history
Syslog History Table: 1 maximum table entries,
saving level Warnings or higher
  SNMP notifications not Enabled
```



```
%RPM:0:0 %CHMGR-2-LINECARDDOWN - Line card 3 down - IPC timeout
Dell#
```

show logging driverlog stack-unit

Display the driver log for the specified stack member.

Syntax	<code>show logging driverlog stack-unit <i>stack-unit-number</i></code>	
Parameters	stack-unit <i>stack-unit-number</i>	Enter the keywords <code>stack-unit</code> followed by the stack member ID of the switch for which you want to display the driver log.
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
9.7(0.0)	Introduced on the S6000-ON.
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.

Usage Information This command displays internal software driver information, which may be useful during troubleshooting switch initialization errors, such as a downed Port-Pipe.

terminal monitor

Configure the Dell Networking OS to display messages on the monitor/terminal.

Syntax	<code>terminal monitor</code> To return to default settings, use the <code>terminal no monitor</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.
E-Series legacy command	

Related Commands [logging monitor](#) — sets the logging parameters on the monitor/terminal.



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.

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 %IFMGR-5-BER_ERR: High Ber detected on interface : %s	SNMP	NONE
BER_ERR_CLR %IFMGR-5-BER_ERR_CLR: High Ber cleared on interface : %s	SNMP	NONE
FAST_RETRAIN %IFMGR-5-FAST_RETRAIN: Retrain event detected on interface : %s	SNMP	NONE
RESV N/A	NONE	NONE
CHM_CARD_DOWN %CHMGR-1-CARD_SHUTDOWN: %sLine card %d down - %s %CHMGR-2-CARD_DOWN: %sLine card %d down - %s	ENVMON	NONE
CHM_CARD_UP %CHMGR-5-LINECARDUP: %sLine card %d is up	ENVMON	NONE
CHM_CARD_MISMATCH %CHMGR-3-CARD_MISMATCH: Mismatch: line card %d is type %s - type %s required.	ENVMON	NONE
CHM_CARD_PROBLEM	ENVMON	NONE
CHM_ALARM_CUTOFF	ENVMON	NONE
CHM_SFM_UP	ENVMON	NONE
CHM_SFM_DOWN	ENVMON	NONE
CHM_RPM_UP %RAM-6-RPM_STATE: RPM1 is in Active State %RAM-6-RPM_STATE: RPM0 is in Standby State	ENVMON	NONE
CHM_RPM_DOWN %CHMGR-2-RPM_DOWN: RPM 0 down - hard reset %CHMGR-2-RPM_DOWN: RPM 0 down - card removed	ENVMON	NONE
CHM_RPM_PRIMARY %RAM-5-COLD_FAILOVER: RPM Failover Completed %RAM-5-HOT_FAILOVER: RPM Failover Completed %RAM-5-FAST_FAILOVER: RPM Failover Completed	ENVMON	NONE
CHM_SFM_ADD %TSM-5-SFM_DISCOVERY: Found SFM 1	ENVMON	NONE



Message ID	Trap Type	Trap Option
CHM_SFM_REMOVE %TSM-5-SFM_REMOVE: Removed SFM 1	ENVMON	NONE
CHM_MAJ_SFM_DOWN %CHMGR-0-MAJOR_SFM: Major alarm: Switch fabric down	ENVMON	NONE
CHM_MAJ_SFM_DOWN_CLR %CHMGR-5-MAJOR_SFM_CLR: Major alarm cleared: Switch fabric up	ENVMON	NONE
CHM_MIN_SFM_DOWN %CHMGR-2-MINOR_SFM: Minor alarm: No working standby SFM	ENVMON	NONE
CHM_MIN_SFM_DOWN_CLR %CHMGR-5-MINOR_SFM_CLR: Minor alarm cleared: Working standby SFM present	ENVMON	NONE
CHM_PWRSRC_DOWN %CHMGR-2-PEM_PRBLM: Major alarm: problem with power entry module %s	ENVMON	SUPPLY
CHM_PWRSRC_CLR %CHMGR-5-PEM_OK: Major alarm cleared: power entry module %s is good	ENVMON	SUPPLY
CHM_MAJ_ALARM_PS %CHMGR-0-MAJOR_PS: Major alarm: insufficient power %s	ENVMON	SUPPLY
CHM_MAJ_ALARM_PS_CLR %CHMGR-5-MAJOR_PS_CLR: major alarm cleared: sufficient power	ENVMON	SUPPLY
CHM_MIN_ALARM_PS %CHMGR-1-MINOR_PS: Minor alarm: power supply non-redundant	ENVMON	SUPPLY
CHM_MIN_ALARM_PS_CLR %CHMGR-5-MINOR_PS_CLR: Minor alarm cleared: power supply redundant	ENVMON	SUPPLY
CHM_MIN_ALRM_TEMP %CHMGR-2-MINOR_TEMP: Minor alarm: chassis temperature	ENVMON	TEMP
CHM_MIN_ALRM_TEMP_CLR %CHMGR-5-MINOR_TEMP_CLR: Minor alarm cleared: chassis temperature normal (%s %d temperature is within threshold of %dC)	ENVMON	TEMP
CHM_MAJ_ALRM_TEMP %CHMGR-2-MAJOR_TEMP: Major alarm: chassis temperature high (%s temperature reaches or exceeds threshold of %dC)	ENVMON	TEMP
CHM_MAJ_ALRM_TEMP_CLR %CHMGR-2-MAJOR_TEMP_CLR: Major alarm cleared: chassis temperature lower (%s %d temperature is within threshold of %dC)	ENVMON	TEMP
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	ENVMON	FAN
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		
CHM_MIN_FANBAD	ENVMON	FAN
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		
CHM_MIN_FANBAD_CLR	ENVMON	FAN
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		
TME_TASK_SUSPEND	ENVMON	NONE
%TME-2-TASK SUSPENDED: SUSPENDED - svce:%d - inst:%d - task:%s		
TME_TASK_TERM	ENVMON	NONE
%TME-2-ABNORMAL_TASK_TERMINATION: CRASH - task:%s %s		
CHM_CPU_THRESHOLD	ENVMON	NONE
%CHMGR-5-CPU_THRESHOLD: Cpu %s usage above threshold. Cpu5SecUsage (%d)		
CHM_CPU_THRESHOLD_CLR	ENVMON	NONE
%CHMGR-5-CPU_THRESHOLD_CLR: Cpu %s usage drops below threshold. Cpu5SecUsage (%d)		
CHM_MEM_THRESHOLD	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD: Memory %s usage above threshold. MemUsage (%d)		
CHM_MEM_THRESHOLD_CLR	ENVMON	NONE
%CHMGR-5-MEM_THRESHOLD_CLR: Memory %s usage drops below threshold. MemUsage (%d)		
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		



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.**

show storm-control broadcast

Display the storm control broadcast configuration.

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/subport 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
9.7(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.
8.5.1.0	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.

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/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.

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
9.7(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.
8.5.1.0	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 1/1/1

Multicast storm control configuration

Interface  Direction      Packets/Second
-----
Te 1/1/1      Ingress           5

Dell#
```

show storm-control unknown-unicast

Display the storm control unknown-unicast configuration.

Syntax `show storm-control unknown-unicast [interface]`

Parameters

<i>interface</i>	(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/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.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.5.1.0	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.

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

<i>percentagedecimal_value in out</i>	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 decimal range is from .1 to .9.
wred-profile name	Enter the keyword wred-profile followed by the profile name to designate a wred-profile.
<i>packets_per_second in</i>	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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.3.11.1	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 <code>percentage decimal value</code> 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).

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
9.7(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.
7.4.1.0	E-Series Only: Added the <code>percentage decimal value</code> 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.

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
9.7(0.0)	Introduced on the S6000-ON.
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 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.

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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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 C-series and S-Series.

storm-control unknown-unicast (Configuration)

Configure the percentage of unknown-unicast traffic allowed in or out of the network.

Syntax	<code>storm-control unknown-unicast [packets_per_second in]</code> To disable storm control for unknown-unicast traffic, use the <code>no storm-control unknown-unicast [packets_per_second in]</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
7.4.1.0	E-Series Only: Added the <code>percentage decimal value</code> option.



Version	Description
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).

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 <code>wred-profile</code> 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
9.7(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.



Version	Description
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.



Spanning Tree Protocol (STP)

The commands in this chapter configure and monitor the IEEE 802.1d spanning tree protocol (STP) and are supported on the Dell Networking switch/routing platform.

bridge-priority

Set the bridge priority of the switch in an IEEE 802.1D spanning tree.

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 <code>primary</code> to designate the bridge as the root bridge.
secondary	Enter the keyword <code>secondary</code> 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
9.7(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.
7.7.1.0	Introduced on the S-Series.
7.5.1.0	Introduced on the C-Series.
6.2.1.1	Introduced on the E-Series.

bpdudestination-mac-address

Use the Provider Bridge Group address in Spanning Tree or GVRP PDUs.

Syntax	<code>bpdudestination-mac-address [stp gvrp] provider-bridge-group</code>	
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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	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.

debug spanning-tree

Enable debugging of the spanning tree protocol and view information on the protocol.

Syntax	<code>debug spanning-tree {stp-id [all bpdud config events exceptions general root] protocol}</code> To disable debugging, use the <code>no debug spanning-tree</code> 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 <code>mstp</code> , <code>pvst</code> , or <code>rstp</code> .
	all	(OPTIONAL) Enter the keyword <code>all</code> to debug all spanning tree operations.
	bpdud	(OPTIONAL) Enter the keyword <code>bpdud</code> to debug bridge protocol data units.
	config	(OPTIONAL) Enter the keyword <code>config</code> to debug configuration information.
	events	(OPTIONAL) Enter the keyword <code>events</code> to debug STP events.
	general	(OPTIONAL) Enter the keyword <code>general</code> to debug general STP operations.
	root	(OPTIONAL) Enter the keyword <code>root</code> 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
9.7(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.
7.7.1.0	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 bpd` 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.

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
9.7(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.
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.

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
9.7(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.
7.7.1.0	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.

Syntax `forward-delay seconds`
To return to the default setting, use the `no forward-delay` command.

Parameters `seconds` Enter the number of seconds the Dell Networking OS 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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	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).

Syntax	<code>hello-time seconds</code>
	To return to the default value, use the <code>no hello-time</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	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.
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.

Syntax `max-age seconds`

To return to the default values, use the `no max-age` command.

Parameters

seconds Enter a number of seconds the Dell Networking OS 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
9.7(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.
7.7.1.0	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.

Syntax	<code>protocol spanning-tree stp-id</code> To disable the Spanning Tree group, use the <code>no protocol spanning-tree stp-id</code> command.																			
Parameters	<i>stp-id</i>	Enter zero (0). Dell Networking OS 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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.7.0</td><td>Introduced on the S4810.</td></tr><tr><td>7.7.1.0</td><td>Introduced on the S-Series.</td></tr><tr><td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr><tr><td>6.2.1.1</td><td>Introduced on the E-Series.</td></tr></table>		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.	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.
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.																			
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 <code>no disable</code> command from SPANNING TREE mode.																			
Example	<pre>Dell (conf) #protocol spanning-tree 0 Dell (config-stp) #</pre>																			
Related Commands	disable — disables spanning tree group 0. To enable spanning tree group 0, use the <code>no disable</code> command.																			

show config

Display the current configuration for the mode. Only non-default values display.

Syntax	<code>show config</code>
Command Modes	SPANNING TREE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . 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.
9.0.2.0	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	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.

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 <code>active</code> to display only active interfaces in spanning tree group 0.
brief	(OPTIONAL) Enter the keyword <code>brief</code> to display a synopsis of the spanning tree group configuration information.
guard	(OPTIONAL) Enter the keyword <code>guard</code> to display the type of guard enabled on an STP interface and the current port state.
interface <i>interface</i>	(OPTIONAL) Enter the keyword <code>interface</code> 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 <code>port-channel</code> then a number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information.
root	(OPTIONAL) Enter the keyword <code>root</code> to display configuration information on the spanning tree group root.
summary	(OPTIONAL) Enter the keyword <code>summary</code> 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, refer to the relevant *Dell 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.
9.0.2.0	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 ExaScale.
8.4.2.1	Added support for the optional <code>guard</code> 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.
"Designated root..."	Displays the priority and MAC address of the root bridge of the STG that the interface belongs.

Field	Description
"Designated port..."	Displays the designated port ID.

Example

```
Dell#show spann 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 1/1/1) 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 1/1/2) 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 1/1/3) 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 1/1/1 8.26 8 4 FWD 0 32768 0001.e800.0a56 8.26
Te 1/1/2 8.27 8 4 FWD 0 32768 0001.e800.0a56 8.27
Te 1/1/3 8.28 8 4 FWD 0 32768 0001.e800.0a56 8.28
Dell#
```



Usage Information The following describes the `show spanning-tree 0 guard` command shown in the example.

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).

Example (Guard)

```
Dell#show spanning-tree 0 guard
Interface
Name      Instance   Sts          Guard type
-----
Te 1/1/1   0          INCON (Root) Rootguard
Te 1/1/2   0          LIS          Loopguard
Te 1/1/3   0          EDS (Shut)   Bpduguard
```

spanning-tree

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.

Syntax

```
spanning-tree stp-id {cost cost | {loopguard | rootguard} | portfast
[bpduguard [shutdown-on-violation]] | priority priority}
```

To disable Spanning Tree group on an interface, use the `no spanning-tree stp-id {cost cost | {loopguard | rootguard} | portfast [bpduguard [shutdown-on-violation]] | priority priority}` command.

Parameters

<i>stp-id</i>	Enter the STP instance ID. The range is 0.
<i>cost cost</i>	Enter the keyword <code>cost</code> then a number as the cost. The range is from 1 to 65535. The defaults are: • 1-Gigabit Ethernet interface = 4. • 10-Gigabit Ethernet interface = 2. • Port Channel interface with 100 Mb/s Ethernet = 18. • Port Channel interface with 1 Gigabit Ethernet = 3. • Port Channel interface with 10 Gigabit Ethernet = 1.
<i>loopguard</i>	Enter the keyword <code>loopguard</code> to enable STP loop guard on a port or port-channel interface.
<i>rootguard</i>	Enter the keyword <code>rootguard</code> to enable STP root guard on a port or port-channel interface.
<i>portfast</i> [bpduguard [shutdown-on-violation]]	Enter the keyword <code>portfast</code> to enable Portfast to move the interface into Forwarding mode immediately after the root fails. Enter the optional keyword <code>bpduguard</code> 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, refer to the relevant *Dell 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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.11.1	Introduced on the Z9000.
8.3.10.1	Introduced the <code>loopguard</code> and <code>rootguard</code> options on the S4810.
8.4.2.1	Introduced the <code>loopguard</code> and <code>rootguard</code> 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 <code>shutdown-on-violation</code> 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.



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*.

The commands in this chapter are generally supported on Dell Networking OS with some exceptions, as notes in the Command History fields.

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.

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

<i>time-zone</i>	Enter the three-letter name for the time zone. This name is displayed in the show clock output.
<i>start-month</i>	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.
<i>start-day</i>	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.
<i>start-year</i>	Enter a four-digit number as the year. The range is from 1993 to 2035.
<i>start-time</i>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
<i>end-day</i>	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.
<i>end-month</i>	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.
<i>end-time</i>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
<i>end-year</i>	Enter a four-digit number as the year. The range is from 1993 to 2035.
<i>offset</i>	(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
9.7(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.
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.

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.



<i>start-month</i>	Enter the name of one of the 12 months in English.
<i>start-time</i>	Enter the time in hours:minutes. For the hour variable, use the 24-hour format; example, 17:15 is 5:15 pm.
<i>end-week</i>	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.
<i>end-day</i>	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.
<i>end-month</i>	Enter the name of one of the 12 months in English.
<i>end-time</i>	Enter the time in hours:minutes:seconds. For the hour variable, use the 24-hour format; example, 17:15:00 is 5:15 pm.
<i>offset</i>	(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
9.7(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.
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.

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
9.7(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.
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 {adjust | all | authentication | events | loopfilter | packets | select | sync}`

To disable debugging of NTP transactions, use the `no debug ntp {adjust | all | authentication | events | loopfilter | packets | select | sync}` command.



Parameters	adjust	Enter the keyword <code>adjust</code> to display information on NTP clock adjustments.
	all	Enter the keyword <code>all</code> to display information on all NTP transactions.
	authentication	Enter the keyword <code>authentication</code> to display information on NTP authentication transactions.
	events	Enter the keyword <code>events</code> to display information on NTP events.
	loopfilter	Enter the keyword <code>loopfilter</code> to display information on NTP local clock frequency.
	packets	Enter the keyword <code>packets</code> to display information on NTP packets.
	select	Enter the keyword <code>select</code> to display information on the NTP clock selection.
	sync	Enter the keyword <code>sync</code> to display information on the NTP clock synchronization.

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
9.7(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.
6.1.1.0	Introduced on the E-Series.

ntp authenticate

Enable authentication of NTP traffic between the switch and the NTP time serving hosts.

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
9.7(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.
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.

ntp broadcast client

Set up the interface to receive NTP broadcasts from an NTP server.

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
9.7(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.
6.1.1.0	Introduced on the E-Series.



ntp disable

Prevent an interface from receiving NTP packets.

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
9.7(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.
6.1.1.0	Introduced on the E-Series.

ntp multicast client

To receive NTP information from the network via multicast, configure the switch.

Syntax `ntp multicast client [multicast-address]`

To disable multicast reception, use the `no ntp multicast client [multicast-address]` command.

Parameters

multicast-address (OPTIONAL) Enter a multicast address. Enter either an IPv4 address in dotted decimal format or an IPv6 address in X:X:X:X format. If you do not enter a multicast address, the address:

- 224.0.1.1 is configured if the interface address is IPv4
- ff05::101 is configured if the interface address is IPv6

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
9.7(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.
8.4.1.0	Added support for IPv6 multicast addresses.
8.3.7.0	Introduced on the S4810.
6.1.1.0	Introduced on the E-Series.

ntp master <stratum>

Configure the switch as NTP Server.

Syntax `ntp master <stratum>`

Parameters

ntp	Enter the <code>stratum</code> number to identify the NTP Server's hierarchy.
master<stratum>	

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.
9.6(0.0)	Introduced on the S4810, S4820T, S5000, S6000, Z9000, and Z9500.

ntp server

Configure an NTP time-serving host.

Syntax `ntp server[vrf vrf-name] {hostname | ipv4-address | ipv6-address} [key
keyid] [prefer] [version number]`



Parameters	vrf <i>vrf-name</i>	(Optional) Enter the keyword <code>vrf</code> and then the name of the VRF to configure a NTP time-serving host corresponding to that VRF.
	<i>ipv4-address</i> <i>ipv6-address</i>	Enter an IPv4 address (A.B.C.D) or IPv6 address (X:X:X:X::X) of NTP server.
	<i>hostname</i>	Enter the hostname of the server.
	key <i>keyid</i>	(OPTIONAL) Enter the keyword <code>key</code> and a number as the NTP peer key. The range is from 1 to 4294967295.
	prefer	(OPTIONAL) Enter the keyword <code>prefer</code> to indicate that this peer has priority over other servers.
	version <i>number</i>	(OPTIONAL) Enter the keyword <code>version</code> and a number to correspond to the NTP version used on the server. The range is from 1 to 4.

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.
9.6(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.
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 Networking OS chooses one NTP host with which to synchronize. To determine which server was selected, use the `show ntp associations` command.

Because many polls to NTP hosts can impact network performance, Dell Networking recommends limiting the number of hosts configured.

Related Commands [show ntp associations](#) — displays the NTP servers 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/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 keyword `lag` then a number. The range is from 1 to 128.
- 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.
9.0.2.0	Introduced on the S6000.
8.3.11.1	Introduced on the Z9000.
8.5.1.0	Added support for 4-port 40G line cards on 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.

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 4294967295.



Defaults	Not configured.														
Command Modes	CONFIGURATION														
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <tr> <th>Version</th><th>Description</th></tr> <tr> <td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr> <tr> <td>9.0.2.0</td><td>Introduced on the S6000.</td></tr> <tr> <td>8.3.11.1</td><td>Introduced on the Z9000.</td></tr> <tr> <td>7.6.1.0</td><td>Introduced on the S-Series.</td></tr> <tr> <td>7.5.1.0</td><td>Introduced on the C-Series.</td></tr> <tr> <td>6.1.1.0</td><td>Introduced on the E-Series.</td></tr> </table>	Version	Description	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.	7.6.1.0	Introduced on the S-Series.	7.5.1.0	Introduced on the C-Series.	6.1.1.0	Introduced on the E-Series.
Version	Description														
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.														
7.6.1.0	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 <code>number</code> parameter in the <code>ntp trusted-key</code> command must be the same number as the <code>number</code> parameter in the <code>ntp authentication-key</code> command. If you change the <code>ntp authentication-key</code> command, you must also change the <code>ntp trusted-key</code> command.														
Related Commands	ntp authentication-key — sets an authentication key for NTP. ntp authenticate — enables the NTP authentication parameters you set.														

ntp authentication-key

Specify a key for authenticating the NTP server.

Syntax	<code>ntp authentication-key <i>number</i> md5 [0 7] <i>key</i></code>	
Parameters	<i>number</i>	Specify a number for the authentication key. The range is from 1 to 4294967295. This number must be the same as the <code>number</code> parameter configured in the <code>ntp trusted-key</code> command.
	<i>md5</i>	Specify that the authentication key is encrypted using MD5 encryption algorithm.
	<i>0</i>	Specify that authentication key is entered in an unencrypted format (default).
	<i>7</i>	Specify that the authentication key is entered in DES encrypted format.
	<i>key</i>	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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	



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.
9.0.2.0	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 Networking OS versions 8.2.1.0 and later use an encryption algorithm to store the authentication key that is different from previous Dell Networking OS versions; beginning in version 8.2.1.0, Dell 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 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.

show clock

Display the current clock settings.

Syntax `show clock [detail]`

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, refer to the relevant *Dell 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.



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.
7.6.1.0	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 (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, refer to the relevant *Dell 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.
9.0.2.0	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
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. • ~ means the peer is statically configured.
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).
disp	Displays the dispersion.

Example

```
Dell#show ntp associations
remote      ref clock  st when poll reach delay  offset disp
=====
 10.10.120.5 0.0.0.0    16 - 256      0 0.00 0.000 16000.0
*172.16.1.33 127.127.1.0 11 6 16      377 -0.08 -1499.9 104.16
 172.31.1.33 0.0.0.0    16 - 256      0 0.00 0.000 16000.0
 192.200.0.2 0.0.0.0    16 - 256      0 0.00 0.000 16000.0
* master (synced), # master (unsynced), + selected, - candidate
Dell#
```

Related Commands [show ntp status](#) — displays the current NTP status.

show ntp vrf associations

Displays the NTP servers configured for the VRF instance <vrf-name>.

Syntax `show ntp [vrf] <vrf-name> 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
9.7(0.0)	Introduced on the S6000-ON.
9.6(0.0)	Added support for VRF.
9.4.(0.0)	Added support for VRF.
9.0.2.0	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.

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, refer to the relevant *Dell 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.
9.0.2.0	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

```
Dell#show ntp status
Clock is synchronized, stratum 2, reference is 100.10.10.10
frequency is -32.000 ppm, stability is 15.156 ppm, precision is 4294967290
reference time is BC242FD5.C7C5C000 (10:15:49.780 UTC Mon Jan 10 2000)
clock offset is clock offset msec, root delay is 0.01656 sec
root dispersion is 0.39694 sec, peer dispersion is peer dispersion msec
peer mode is client
Dell#
```

Related Commands [show ntp associations](#) — displays information on the NTP master and peer configurations.



Tunneling

Tunneling is supported on Dell Networking OS.

ip unnumbered

Configure a tunnel interface to operate without a unique IPv4 address and select the interface from which the tunnel borrows its address.

Syntax `ip unnumbered {interface-type slot/port[/subport]}`

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

<i>interface-type</i>	Enter the interface type, followed by a slot number.
<i>interface-number</i>	

Defaults None

Command Modes INTERFACE TUNNEL

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
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.

Syntax	ipv6 unnumbered <i>{interface-type interface-number}</i>											
	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	<i>interface-type</i> <i>interface-number</i>	Enter the interface type, followed by the type, slot and port information.										
Defaults	None.											
Command Modes	INTERFACE TUNNEL											
Command History	<table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.4(0.0)</td><td>Introduced on the S4810, S4820T.</td></tr><tr><td>9.3(0.1)</td><td>Introduced on the S6000 and Z9000.</td></tr></table>	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 S4810, S4820T.	9.3(0.1)	Introduced on the S6000 and Z9000.	
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 S4810, S4820T.											
9.3(0.1)	Introduced on the 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 <code>ipv6 unnumbered</code> 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.

Syntax	tunnel allow-remote { <i>ip-address</i> <i>ipv6-address</i> } [<i>mask</i>]	
	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	<i>ip-address</i>	Enter the source IPv4 address in A.B.C.D format.
	<i>ipv6-address</i>	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
	9.7(0.0)	Introduced on the S6000-ON.
	9.4(0.0)	Introduced on the S4810, S4820T, S6000 and Z9000.
	9.3(0.1)	Introduced on the 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.

Syntax `tunnel destination {ip-address | ipv6-address}`

To delete a tunnel destination address, use the `no tunnel destination {ip-address | ipv6-address}` command.

Parameters

<i>ip-address</i>	Enter the destination IPv4 address for the tunnel.
<i>ipv6-address</i>	Enter the destination IPv6 address for the tunnel.

Defaults none

Command Modes INTERFACE TUNNEL (conf-if-tu)

Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.5(0.1)	Introduced on the Z9500.
	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	<code>tunnel dscp {mapped value}</code>	
	To use the default tunnel mapping behavior, use the <code>no tunnel dscp value</code> command.	
Parameters	mapped	Enter the keyword <code>mapped</code> 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.

Syntax	<code>tunnel flow-label value</code>
	To return to the default value of 0, use the <code>no tunnel flow-label value</code> command.



Parameters	<i>value</i>	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
	9.7(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 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.

Syntax	<code>tunnel hop-limit <i>value</i></code>	To restore the default tunnel hop-limit, use the <code>no tunnel hop-limit</code> command.
Parameters	<i>value</i>	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
	9.7(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	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.

Syntax	<code>tunnel keepalive {<i>ip-address</i> <i>ipv6-address</i>}[interval {<i>seconds</i>}] [<i>attempts</i> {<i>count</i> unlimited}]</code>



To disable the tunnel keepalive probes use the **no tunnel keepalive** command.

Parameters

<i>ip-address ipv6 address</i>	Enter the IPv4 or IPv6 address of the peer to which the keepalive probes will be sent.
<i>interval seconds</i>	Enter the keyword <code>interval</code> 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.
<i>count</i>	(OPTIONAL) Enter the keyword count to count packets processed by the filter. The range is from 3 to 10. The default is 3.
<i>unlimited</i>	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
9.7(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

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.

.

Syntax

```
tunnel mode {ipip | ipv6 | ipv6ip}[decapsulate-any]
```

To disable an active tunnel interface, use the **no tunnel mode** command.



Parameters	<i>ipip</i>	Enable tunnel in RFC 2003 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv4 tunnel.
	<i>ipv6</i>	Enable tunnel in RFC 2473 mode and encapsulate IPv4 and/or IPv6 datagrams inside an IPv6 tunnel.
	<i>ipv6ip</i>	Enable tunnel in RFC 4213 mode and encapsulate IPv6 datagrams inside an IPv4 tunnel.
	<i>decapsulate-any</i>	(Optional) Enable tunnel in multipoint receive-only mode.
Defaults	There is no default tunnel mode.	
Command Modes	INTERFACE TUNNEL	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.5(0.1)	Introduced on the Z9500.
	9.4(0.0)	Added the decapsulate-any command.
	9.3(0.1)	Introduced on the S6000 and Z9000.
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 <code>tunnel-mode</code> 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.

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	<i>ip-address</i>	Enter the source IPv4 address in A.B.C.D format.
	<i>ipv6-address</i>	Enter the source IPv6 address in X:X:X:X format.
	<i>interface-type-number</i>	- For a port channel interface, enter the keywords <code>port-channel</code> then a number from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> 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
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added the tunnel source <code>anylocal</code> command.
9.3(0.0)	Introduced on the S4810, S4820T, S6000 and Z9000.

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**.



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.

The Dell Networking operating software supports this feature on Dell Networking OS.

For more information about basic VLAN commands, refer to 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, refer to [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 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. Refer to [portmode hybrid](#).

dei enable

Make packets eligible for dropping based on their DEI value.

Syntax `dei enable`

Defaults Packets are colored green; no packets are dropped.

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.
9.0.2.0	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 C-Series and S-Series.

dei honor

Honor the incoming DEI value by mapping it to an Dell Networking OS drop precedence. Enter the command once for 0 and once for 1.

Syntax `dei honor {0 | 1} {green | red | yellow}`

Parameters

0 | 1 Enter the bit value you want to map to a color.

green | red | yellow Choose a color:

- **Green:** High priority packets that are the least preferred to be dropped.
- **Yellow:** Lower priority packets that are treated as best-effort.
- **Red:** Lowest priority packets that are always dropped (regardless of congestion status).

Defaults Disabled; Packets with an unmapped DEI value are colored green.

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
9.7(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.
8.3.1.0	Introduced on the C-Series and S-Series.

Usage Information You must first enable DEI for this configuration to take effect.



dei mark

Set the DEI value on egress according to the color currently assigned to the packet.

S6000-ON

Syntax `dei mark {green | yellow} {0 | 1}`

Parameters

`0 | 1`

Enter the bit value you want to map to a color.

`green | red | yellow`

Choose a color:

- **Green:** High priority packets that are the least preferred to be dropped.
- **Yellow:** Lower priority packets that are treated as best-effort.

Defaults

All the packets on egress are marked with DEI 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
9.7(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.
8.3.1.0	Introduced on the C-Series and S-Series.

Usage Information

You must first enable DEI for this configuration to take effect.

member

Assign a stackable VLAN access or trunk port to a VLAN. The VLAN must contain the `vlan-stack compatible` command in its configuration.

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/subport 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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
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.

stack-unit stack-group

Configure a stacking group specified by an ID.

Syntax `[no] stack-unit unit-id stack-group stack-group-id`

Parameters

<i>unit-id</i>	Enter the stack unit ID.
<i>stack-group-id</i>	Enter the stack group ID. The range is from 0 to 16.
<code>[no]</code>	Use <code>no stack-unit unit-id stack-group stack-id</code> to remove the current stack group configuration.

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.10.2	Introduced on the S4810.



Usage Information



WARNING: The following message displays to confirm the command: All non-default configurations on the related member ports ports (<ports listed here>) will be removed. Do you want to continue (y/n)? If you enter “y”, all non-default configurations on any member ports of the current stack group is removed when the unit is rebooted.

vlan-stack access

Specify a Layer 2 port or port channel as an access port to the stackable VLAN network.

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
9.7(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 E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.
E-Series original Command	

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.

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
9.7(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 E-Series ExaScale.
7.6.1.0	Introduced on the C-Series and S-Series.
E-Series original Command	

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.

If VRF is enabled, then you cannot enable the stacked VLAN feature using this command.

If IGMP snooping is enabled, then you cannot enable the stacked VLAN feature using this command.

Example

```
Dell#show vlan
Codes: * - Default VLAN, G - GVRP VLANs

  NUM  Status  Q Ports
*  1    Inactive
  2    Active   M Te 1/13/1
                        M Te 1/1/1-1/1/3
  3    Active   M Pol(Te 1/14/1-1/14/2)
                        M Te 1/18/1
                        M Te 1/4/1
  4    Active   M Pol(Te 1/14/1-1/14/2)
                        M Te 1/18/1
                        M Te 1/5/1
  5    Active   M Pol(Te 1/14/1-1/14/2)
                        M Te 1/18/1
                        M Te 1/6/1
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.

Syntax	<code>vlan-stack dot1p-mapping c-tag-dot1p values sp-tag-dot1p value</code>	
Parameters	c-tag-dot1p value	Enter the keyword <code>c-tag-dot1p</code> then the customer dot1p value that is mapped to a service provider dot1p value. The range is from 0 to 7.
	sp-tag-dot1p value	Enter the keyword <code>sp-tag-dot1p</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.7.0	Introduced on the S4810.
8.3.1.0	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, Dell Networking OS assigns the value 0x9100.

Syntax	<code>vlan-stack protocol-type number</code>	
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, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	

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.
9.0.2.0	Introduced on the S6000.
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.
E-Series original Command	

Usage Information For specific interoperability limitations regarding the S-Tag TPID, refer to 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.

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 Networking OS version history for this command.



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 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.
E-Series original Command	

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.

Starting with Dell Networking OS version 7.8.1.0, 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 “Gi 3/10” port is configured to act as a VLAN-Stack access port, while the “TenGi 8/0” 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-1/23/1)#switchport
Dell(conf-if-te-1/23/1)#vlan-stack trunk
Dell(conf-if-te-1/23/1)#show config
!
interface TenGigabitEthernet 1/23/1
    no ip address
    switchport
    vlan-stack trunk
    no shutdown
Dell(conf-if-te-1/23/1)#interface vlan 100
Dell(conf-if-vl-100)#vlan-stack compatible
Dell(conf-if-vl-100-stack)#member tengigabitethernet 1/23/1
Dell(conf-if-vl-100-stack)#show config
!
interface Vlan 100
    no ip address
    vlan-stack compatible
    member TenGigabitEthernet 1/23/1
    shutdown
Dell(conf-if-vl-100-stack)#interface vlan 20
Dell(conf-if-vl-20)#tagged Tengigabitethernet 1/23/1
Dell(conf-if-vl-20)#show config
```



```

!
interface Vlan 20
  no ip address
  tagged TenGigabitEthernet 1/23/1
  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 1/23/1
  100   Active                M Te 1/23/1
Dell(conf-if-vl-20)#

```

Example 2

```

Dell(config)#vlan-stack protocol-type 88A8
Dell(config)#interface TenGigabitEthernet 3/10/1
Dell(conf-if-te-3/10/1)#no shutdown
Dell(conf-if-te-3/10/1)#switchport
Dell(conf-if-te-3/10/1)#vlan-stack access
Dell(conf-if-te-3/10/1)#exit

Dell(config)#interface TenGigabitEthernet 5/1/1
Dell(conf-if-te-5/1/1)#no shutdown
Dell(conf-if-te-5/1/1)#portmode hybrid
Dell(conf-if-te-5/1/1)#switchport
Dell(conf-if-te-5/1/1)#vlan-stack trunk
Dell(conf-if-te-5/1/1)#exit

Dell(config)#interface vlan 10
Dell(conf-if-vlan)#vlan-stack compatible
Dell(conf-if-vlan)#member Te 4/1/1, Te 3/10/1, TenGi 5/1/1
Dell(conf-if-vlan)#exit

Dell(config)#interface vlan 30
Dell(conf-if-vlan)#untagged TenGi 5/1/1
Dell(conf-if-vlan)#exit
Dell(config)#

Dell(config)#interface vlan 40
Dell(conf-if-vlan)#tagged TenGi 5/1/1
Dell(conf-if-vlan)#exit
Dell(config)#

```



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.

Syntax	<code>ip unknown-unicast</code> 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 <code>no ip unknown-unicast</code> command.	
Defaults	None	
Parameters	<code>vrf vrf-name</code>	(Optional) Enter the keyword <code>vrf</code> followed by the name of the VRF to enable catch-all routes corresponding to that VRF.
Command Modes	CONFIGURATION	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.4(0.0)	Introduced on the S-Series.
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 <code>no ip unknown-unicast</code> command previously. This will be the default configuration after reload.	

ipv6 unknown-unicast

Disable soft forwarding of unknown IPv6 destination packets.

Syntax	<code>[no] ipv6 unknown-unicast</code>
Defaults	Soft forwarding is enabled.
Command Modes	CONFIGURATION



Command History	Version	Description
	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

Enables you to specify a descriptive name for a customer VRF.

Syntax	<code>description string</code>	
	To delete the descriptive name for a customer VRF, use the <code>no description string</code> command.	

Parameters	<i>string</i>	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 <i>Dell Networking OS Command Line Reference Guide</i> .

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(0.0)	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

Enables you to attach an interface to a VRF.

Syntax	<code>ip vrf forwarding {vrf-name management}</code>	
	To delete an interface associated with a configured VRF, use the <code>no ip vrf forwarding {vrf-name management}</code> command.	

Parameters	<i>vrf-name</i>	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, refer to the relevant *Dell 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 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.

Example

```
Dell#configure terminal
Dell(conf)#ip vrf red
Dell(conf-vrf)#description "Red Network"
Dell(conf-vrf)#show config
!
ip vrf red 4
description "Red Network"
Dell(conf-vrf)#

Dell(conf-if-te-1/4/1)#int te 1/4/2
Dell(conf-if-te-1/4/2)#no shut
Dell(conf-if-te-1/4/2)#ip vrf forwarding red
Dell(conf-if-te-1/4/2)#ip add 100.1.1.1/24
Dell(conf-if-te-1/4/2)#
Dell(conf-if-te-1/4/2)#
Dell(conf-if-te-1/4/2)#
Dell(conf-if-te-1/4/2)#show config
!
interface TenGigabitEthernet 1/4/2
ip vrf forwarding red
ip address 100.1.1.1/24
no shutdown
Dell(conf-if-te-1/4/2)#
```



ip http vrf

Configures an HTTP client with a VRF that is used to connect to the HTTP server.

S6000-ON

Syntax	<code>ip http vrf {management vrf-name}</code> To undo the HTTP client configuration, use the <code>ip http vrf</code> command.	
Parameters	management	Enter the keyword <code>management</code> for configuring the management VRF that uses an HTTP client.
	vrf-name	Enter the name of the VRF for configuring a nondefault that uses an HTTP client.
Defaults	Disabled	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> . The following is a list of the Dell Networking OS version history for this command.	
	Version	Description
	9.8(0.0)	Introduced on the S4810, S4820T, S5000, S6000, S6000-ON, and Z9500.
Usage Information	To make the HTTP clients VRF-aware, use the <code>ip http vrf</code> command. The HTTP client uses the VRF name that you specify to reach the HTTP server. If you do not specify a VRF name, then the HTTP client uses the default VRF.	

ip route-export

Enables route leaking between VRFs. Exports or shares IPv4 routes corresponding to one VRF with other non-default VRFs.

Syntax	<code>ip route-export tag [route-map-name]</code>	
Parameters	route-export	Enter the 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 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
9.7(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 can be exposed for leaking. However, you can configure multiple route-import targets because a VRF can accept 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. Meaning, 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 [ip route-import](#) – imports routes from another VRF.

ip route-import

Imports IPv4 routes that are leaked by another VRF using the tag specified by that VRF during export of these routes.

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

N/A

Command Modes

CONFIGURATION

VRF MODE



Command History	Version	Description
	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	ip route-export – exports routes to another VRF.	

ipv6 route-export

Enables route leaking between VRFs. Exports or shares IPv6 routes corresponding to one VRF with other non-default VRFs.

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
	9.7(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 can be exposed for leaking. However, you can configure multiple route-import targets because a VRF can accept 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. Meaning, 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

Imports IPv6 routes that are leaked by another VRF using the tag specified by that VRF during export of these routes.

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.

Defaults N/A

Command Modes

VRF MODE
CONFIGURATION

Command History

Version	Description
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

Enables you to specify matching criteria while exporting or importing routes.

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.
Defaults	N/A	
Command Modes	ROUTE MAP MODE	
Command History	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

Redistributes leaked or exported routes corresponding to specific protocols.

Syntax	<code>redistribute {imported-bgp import-ospf import-isis}</code>	
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.
Defaults	N/A	
Command Modes	CONFIGURATION	
Command History	Version	Description
	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

Associates a management port with a management VRF.

Syntax	<code>interface management</code> To delete the association between a management port and a management VRF, use the <code>no interface management</code> command.
Defaults	None.
Command Modes	VRF MODE
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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(0.0)	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.

Syntax	<code>maximum dynamic-routes limit {warn-threshold threshold-value warning-only}</code> To remove the limit on the maximum number of routes used, use the <code>no maximum dynamic-routes</code> command.						
Parameters	<table><tr><td><i>limit</i></td><td>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).</td></tr><tr><td>warning-threshold</td><td>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.</td></tr><tr><td>warning-only</td><td>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.</td></tr></table>	<i>limit</i>	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.
<i>limit</i>	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 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 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

Displays information corresponding to the VRFs that are configured in the system.

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, refer to the relevant *Dell 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.
9.4(0.0)	Introduced on the S-Series and Z9000.

Example

```
show ip vrf
VRF-Name          VRF-ID  Interfaces
default           0       Te 1/1/1-1/3/1,1/8/1-1/4/7,
                  Fo 1/9/1,1/7/1,1/8/1,1/10/2,
                  Ma 1/1,
                  Ma 2/1,
                  Ma 3/1,
                  Ma 4/1,
                  Ma 5/1,
                  Ma 6/1,
Nu 0,
test1              1       Vl 1
                  Te 1/25/1,1/28/4-1/29/3
test2              2       Te 1/32/1
```




```

FTOS#show ip vrf test1
VRF-Name                VRF-ID Interfaces
test1                    1          Te 1/29/4,1/30/1-1/31/3

```

show run vrf

Displays configuration information corresponding to all the VRFs in the system.

Syntax `show run vrf vrf-name`

Parameters

vrf <i>vrf-name</i>	Enter the keyword <code>vrf</code> 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
9.7(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 "Banking Customer Chennai"

```

Related Commands



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 Layer 3 (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*.

proxy-gateway lldp

Enables the proxy-gateway feature using LLDP protocol.

S6000-ON

Syntax [no] proxy-gateway lldp

Command Modes VLT DOMAIN

Command History

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
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 static

Enables the proxy-gateway feature using static configurations.

S6000-ON

Syntax [no] proxy-gateway static

Command Modes VLT DOMAIN

Command History	Version	Description
	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 <code>proxy-gateway static</code> mac configured is deleted from the Layer 2 module.	
Example	<pre>Dell(conf)#vlt-domain 1 Dell(conf-vlt-domain#proxy-gateway static</pre>	

remote-mac-address exclude-vlan

Configure the proxy-gateway static entry and exclude a VLAN or a range of VLANs from proxy routing.

S6000-ON

Syntax	<code>[no] remote-mac-address mac-address [exclude-vlan vlan-range]</code>	
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
	9.7(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	<pre>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</pre>	



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.

S6000-ON

Syntax	<code>[no] peer-domain-link port-channel <i>interface-identifier</i> exclude-vlan <i>vlan-range</i></code>	
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
	9.7(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	<pre>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</pre>	

proxy-gateway peer-timeout

Enables the VLT node to timeout the transmission of peer's mac address, when the VLT peer is down.

S6000-ON

Syntax	<code>[no] peer-timeout <i>value</i></code>	
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
	9.7(0.0)	Introduced on the S6000-ON.
	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	When a VLT peer goes down, the local VLT node must stop sending its peer's MAC address. If this timeout is configured, the local VLT node will send its peer's MAC address, till the timer expires. By default this timer value is infinity. This timer comes into play, only when the vlt-peer-mac transmit is enabled. Square VLT Topology with single link connecting to the remote peers, is a typical use case for this configuration.	
Example	<code>Dell(conf-vlt-domain-proxy-gw-lldp)# peer-timeout 5</code>	

vlt-peer-mac transmit

Enables the device to transmit, the peer's MAC address along with its own mac-address in the LLDP TLV packets, to the remote VLT Domain.

S6000-ON

Syntax	<code>[no] vlt-peer-mac transmit</code>	
Command Modes	VLT DOMAIN PROXY GW LLDP	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	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 will send only its own MAC address to the remote VLT domain. This configuration is applicable only for a LLDP proxy gateway. Square VLT Topology with single link connecting to the remote peers, is a typical use case for this configuration.	
Example	<code>Dell(conf-vlt-domain-proxy-gw-lldp)# vlt-peer-mac transmit</code>	

show vlt-proxy-gateway

Display the VLT proxy gateway configuration.

S6000-ON

Syntax	<code>show vlt-proxy-gateway [info] {lldp static}</code>	
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
9.7(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
```



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 if any of the following become **TRUE**:

- After making the CLI configuration change, the VLT Unit-Id becomes identical on both peers.
- After making the CLI configuration change, the VLT System-MAC do not match on both peers.

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 if you configure the Unit-Id or System-MAC on only one of the VLT peers.

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.

Syntax	<code>back-up destination {[ipv4-address] [ipv6 ipv6-address] [interval seconds]}</code>	
Parameters	<i>ipv4-address</i>	Enter the IPv4 address of the backup destination.
	<i>ipv6</i>	Enter the keyword <code>ipv6</code> then an IPv6 address in the X:X:X:X::X format.
	<i>interval seconds</i>	Enter the keyword <code>interval</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.

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
9.7(0.0)	Introduced on the S6000-ON.
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 <code>multicast</code> and <code>ndp</code> parameters.



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.
8.3.12.0	Introduced on the S4810.

Example

```
VLT ARP Statistics
-----
ARP Tunnel Pkts sent:0
ARP Tunnel Pkts Rcvd:0
ARP-sync Pkts Sent:0
ARP-sync Pkts Rcvd:0
ARP Reg Request sent:19
ARP Reg Request rcvd:10
```

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.

Syntax `delay-restore`

Parameters

delay-restore	Enter the amount of time, in seconds, to delay bringing up the VLT ports after the VLTi 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
9.7(0.0)	Introduced on the S6000-ON.
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.
- if the Peer VLT device was up at the time the VLTi link failed to the time when it was restored.

Related Commands [show vlt statistics](#) — displays statistics on VLT operations.

delay-restore abort-threshold

Increase the Boot Up timer to some value (>60 seconds).

Syntax	<pre>delay-restore abort-threshold <interval></pre> To remove use the <code>no delay-restore abort-threshold</code> command.				
Defaults	60 seconds				
Command Modes	VLT DOMAIN				
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table> <thead> <tr> <th>Version</th><th>Description</th></tr> </thead> <tbody> <tr> <td>9.7(0.0)</td><td>Introduced on the S4820T, S4810, S6000, S5000, Z9000, S6000–ON and Z9500.</td></tr> </tbody> </table>	Version	Description	9.7(0.0)	Introduced on the S4820T, S4810, S6000, S5000, Z9000, S6000–ON and Z9500.
Version	Description				
9.7(0.0)	Introduced on the S4820T, S4810, S6000, S5000, Z9000, S6000–ON and Z9500.				
Parameter	Enter the value (in seconds) to specify the time interval for delay restore timer to abort. This timer is applicable only during reload/boot-up and not in other scenarios (example, ICL flap). The range is from 1 to 1800 seconds.				
Usage Information	To abort VLT delay restore timer as the maximum threshold, the maximum time interval is applied to hold down ICL peer-up in the start-up configurations during the reload.				

lACP ungroup member-independent

Prevent possible loop during the bootup of a VLT peer switch or a device that accesses the VLT domain.

Syntax	lACP ungroup member-independent {vlt port-channel}					
Parameters	<table><tr><td>port-channel</td><td>Force all LACP port-channel members to become switchports.</td></tr><tr><td>vlt</td><td>Force all VLT LACP members to become switchports.</td></tr></table>		port-channel	Force all LACP port-channel members to become switchports.	vlt	Force all VLT LACP members to become switchports.
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 <i>Dell Networking OS Command Line Reference Guide</i> .					



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.
9.2(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.

On the S4810, during boot-up in a stacking configuration, the system must be able to reach the DHCP server with the boot image and configuration image. During boot-up, only untagged DHCP requests are sent to the DHCP server to receive an offer on static LAGs between switches. The DHCP server must be configured to start in BMP mode. If switches are connected using LACP port-channels like the VLT peer and Top of Rack (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.

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.

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.

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
9.7(0.0)	Introduced on the S6000-ON.
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.

Syntax `peer-link port-channel port-channel-number {peer-down-vlan vlan id}`

Parameters

<i>port-channel-number</i>	Enter the port-channel number that acts as the interconnect trunk. The range is from 1 to 128.
<i>peer-down-vlan vlan id</i>	Enter the keyword <code>peer-down-vlan</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.

Syntax	<code>peer-routing</code> To disable L3 VLT peer-routing, use the <code>no peer-routing</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .

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)	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.
9.2(0.2)	Introduced 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. If not configured, peer-routing will not be disabled at all even though the peer is unavailable.

Syntax	<code>peer-routing-timeout value</code> To restore the default value, use the <code>no peer-routing-timeout</code> command.		
Parameters	<table><tr><td>value</td><td>Enter the timeout value in seconds. The range is from 1 to 65535. The default value is infinity.</td></tr></table>	value	Enter the timeout value in seconds. The range is from 1 to 65535. The default value is infinity.
value	Enter the timeout value in seconds. The range is from 1 to 65535. The default value is infinity.		
Command Modes	VLT DOMAIN (conf-vlt-domain)		
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .		

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.
9.7(0.0)	Added support for default value on the S-Series and Z-Series.
9.5(0.1)	Introduced on the Z9500.
9.4(0.0)	Added the support for IPV6 / IPV4.



Version	Description
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.

Syntax [no] primary-priority

Parameters **value** To configure the primary role on a VLT peer, 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
9.7(0.0)	Introduced on the S6000-ON.
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 the VLT domain on each peer switch on both sides of the interconnect trunk, by default, the Dell Networking OS software elects a primary and secondary VLT peer device. To reconfigure the primary role of VLT peer switches, use the `priority` command.

show vlt brief

Displays summarized status information about VLT domains currently configured on the switch.

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
9.7(0.0)	Introduced on the S6000-ON.
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.

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#show vlt br
VLT Domain Brief
-----
Domain ID                : 1
Role                     : Secondary
Role Priority             : 32768
ICL Link Status          : Up
HeartBeat Status         : Up
VLT Peer Status          : Up
Version                  : 6(3)
Local System MAC address : 00:01:e8:8a:e9:91
Remote System MAC address : 00:01:e8:8a:e9:76
Remote system version    : 6(3)
Delay-Restore timer      : 90 seconds

Delay-Restore Abort Threshold : 60 seconds
Peer-Routing                  : Disabled
Peer-Routing-Timeout timer   : 0 seconds
Multicast peer-routing timeout : 150 seconds
Dell#
```

show vlt backup-link

Displays information on the backup link operation.

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
9.7(0.0)	Introduced on the S6000-ON.
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.

Syntax `show vlt counters [arp| igmp-snoop | interface | mac | ndp]`

Parameters

arp	Enter the keyword <code>arp</code> to display the ARP counter information for the VLT.
igmp-snoop	Enter the keywords <code>igmp-snoop</code> to display the igmp-snooping counter information for the VLT.
interface	Enter the keyword <code>interface</code> to display the interface counter information for the VLT.
mac	Enter the keyword <code>mac</code> to display the MAC address counter information for the VLT.
ndp	Enter the keyword <code>ndp</code> 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
9.7(0.0)	Introduced on the S6000-ON.
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.
8.3.12.0	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 domains currently configured on the switch.

Syntax show vlt detail

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
9.7(0.0)	Introduced on the S6000-ON.
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# Dell(conf-if-vl-100)#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.

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
9.7(0.0)	Introduced on the S6000-ON.
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 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)
Dell#
```

```
VLAN 15
```

```
te 1/5/1
```

show vlt mismatch

Display mismatches in VLT parameters.

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
9.7(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 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.

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
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.
9.0.2.0	Introduced on the S6000.



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.

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.

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
9.7(0.0)	Introduced on the S6000-ON.
9.5(0.1)	Introduced on the Z9500.



Version	Description
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.
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

```

show vlt statistics igmp-snoop

Displays the informational packets and IGMP control PDUs that are exchanged between VLT peer nodes.

Syntax	<code>show vlt statistics igmp-snoop</code>
Default	Not configured.
Command Modes	EXEC
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .

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.
9.0.2.0	Introduced on the S6000.
8.3.19.0	Introduced on the S4820T.
8.3.12.0	Introduced on the S4810.

Example

```

Dell_VLTpeer1#show vlt statistics igmp-snoop
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

```

unit-id

Explicitly configure the default unit ID of a VLT peer switch.

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 <i>Dell Networking OS Command Line Reference Guide</i>. The following is a list of the Dell Networking OS version history for this command. <table><tr><th>Version</th><th>Description</th></tr><tr><td>9.7(0.0)</td><td>Introduced on the S6000-ON.</td></tr><tr><td>9.5(0.1)</td><td>Introduced on the Z9500.</td></tr><tr><td>9.2(0.0)</td><td>Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.</td></tr><tr><td>9.0.2.0</td><td>Introduced on the S6000.</td></tr><tr><td>9.0.0.0</td><td>Introduced on the Z9000.</td></tr><tr><td>8.3.19.0</td><td>Introduced on the S4820T.</td></tr><tr><td>8.3.8.0</td><td>Introduced on the S4810.</td></tr></table>		Version	Description	9.7(0.0)	Introduced on the S6000-ON.	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.
Version	Description																	
9.7(0.0)	Introduced on the S6000-ON.																	
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 <code>unit-id</code> 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.

Syntax	<code>vlt domain domain-id</code>	
Parameters	<i>domain-id</i>	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 <i>Dell Networking OS Command Line Reference Guide</i>. 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.
9.2(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.

Syntax `vlt-peer-lag port-channel id-number`

Parameters

<i>id-number</i>	Enter the respective vlt port-channel number of the peer device. The range is from 1 to 128.

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
9.7(0.0)	Introduced on the S6000-ON.
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.
9.2(0.0)	Introduced on the M I/O Aggregator. This command is supported in Programmable-Mux (PMUX) mode only.



Virtual Extensible LAN (VXLAN)

Virtual Extensible LAN (VXLAN) is supported on Dell Networking OS.

feature vxlan

Enable VXLAN configuration globally on the platform.

Syntax	<code>feature vxlan</code> To disable the VXLAN, use the <code>no feature vxlan</code> command.	
Defaults	Disabled	
Command Modes	CONFIGURATION	
Command History	This guide is platform-specific. For command information about other platforms, refer to the relevant <i>Dell Networking OS Command Line Reference Guide</i> .	
	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.4(0.0)	Introduced on the S6000.
Usage Information	You must configure feature VXLAN to configure VXLAN-instance.	
Related Commands	vxlan-instance — Enable VXLAN Instance configuration on the platform.	

debug vxlan

Debug messages between the Gateway and Controller.

Syntax	<code>debug vxlan</code>	
Defaults	Disabled	
Command Modes	EXEC Privilege	
Command History	Version	Description
	9.7(0.0)	Introduced on the S6000-ON.
	9.4(0.0)	Introduced on the S6000.



fail-mode

Configures failure-mode on the platform.

Syntax `fail-mode secure`

To disable the `fail-mode secure`, use the `no fail-mode secure` command.

Parameters

secure Enter the keyword `secure` to delete all its database and hardware flows/resources, when the VTEP loses connectivity with the controller.

Defaults `non secure`

Command Modes `VXLAN INSTANCE`

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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S6000.

Related Commands [vxlan-instance](#)— Enable VXLAN Instance configuration on the platform.

vxlan-instance

Enable VXLAN Instance configuration on the platform.

Syntax `vxlan-instance instance ID`

To enable the `vxlan-instance` command, use the `[no] shut` command.

To delete `vxlan-instance` from the system, use `no vxlan-instance 1` command.

Parameters

instance ID Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.

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*.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S6000.

Usage Information You must configure VXLAN globally before using VXLAN-instance.



Related Commands [feature vxlan](#) — Enable VXLAN configuration globally on the platform.

vxlan-instance (VAP)

To configure a VXLAN-Access Port (VAP) in to VXLAN-instance

Syntax `vxlan-instance instance ID`
To unconfigure VAP, use the `no vxlan-instance 1` command.

Parameters **instance ID** Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.

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*.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S6000.

Usage Information You must disable `vxlan-instance` before unconfiguring VAP.

Related Commands [feature vxlan](#) — Enable VXLAN configuration globally on the platform.

max_backoff

Configures time to wait between connection attempts with controller.

Syntax `max_backoff time`

Parameters **time** Enter the time in milliseconds. The range is from 1000-180000. The default value is 30000.

Defaults 30000

Command Modes VXLAN INSTANCE

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
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S6000.



Usage Information The retry interval value caps at the value configured on the max-backoff.

Related Commands [vxlan-instance](#) — Enable VXLAN Instance configuration on the platform.

gateway-ip

Configures gateway IP address on the platform.

Syntax `gateway-ip IP address`

Parameters

<i>IP address</i>	Enter the IP address of the gateway for the VXLAN instance.

Defaults Disabled

Command Modes VXLAN INSTANCE

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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S6000.

Related Commands [vxlan-instance](#) — Enable VXLAN Instance configuration on the platform.

controller

Configures controller for the VXLAN instance on the platform.

Syntax `controller controller ID ip address port port-number tcp|ptcp|pssl|ssl`

Parameters

<i>controller ID</i>	Enter the controller ID.
<i>ip address</i>	Enter the IP address of the controller.
<i>port port-number</i>	(OPTIONAL) Enter the keyword <code>port</code> and the port number. The range is from 1 to 6632. The default port number is 6632.
tcp	(OPTIONAL) Enter the keyword <code>tcp</code> to configure tcp connection to controller.
ptcp	(OPTIONAL) Enter the keyword <code>ptcp</code> to configure passive tcp connection to controller.
pssl	(OPTIONAL) Enter the keyword <code>pssl</code> to configure passive ssl connection to controller.
ssl	(OPTIONAL) Enter the keyword <code>ssl</code> to configure ssl connection to controller (Default).

Defaults Disabled



Command Modes VXLAN INSTANCE

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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S6000.

Related Commands [vxlan-instance](#) — Enable VXLAN instance configuration on the platform.

show vxlan vxlan-instance

Displays information related to Network Virtualization Overlay (NVO) Gateway.

Syntax `show vxlan vxlan-instance instance ID`

Parameters

<i>instance ID</i>	Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.

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
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S6000.

Example

```
Dell#show vxlan vxlan-instance 1
Instance           : 1
Admin State        : enabled
Management IP      : 192.168.200.200
Gateway IP         : 3.3.3.3
MAX Backoff        : 30000
Controller 1       : 192.168.122.6:6632 ssl (connected)
Fail Mode          : secure
Port List          :
Fo 1/4             Te 1/16   Te 1/20   Po 2
```

Related Commands [vxlan-instance](#)- Enable VXLAN Instance configuration on the platform.



show running-config vxlan

Displays the VXLAN configuration information from running configuration.

Syntax `show running-config vxlan`

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
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S6000.

Example

```
Dell#show running-config vxlan
!
feature vxlan
!
vxlan-instance 1
gateway-ip 3.3.3.3
fail-mode secure
controller 1 192.168.122.6 port 6632 ssl
no shutdown
```

Related Commands [vxlan-instance](#)- Enable VXLAN Instance configuration on the platform.

show vxlan vxlan-instance unicast-mac-remote

Displays the information of the remote unicast MACs associated with the logical network related to Network Virtualization Overlay (NVO) Gateway.

Syntax `show vxlan vxlan-instance instance ID unicast-mac-remote [logical-network name | vnid VNID]`

Parameters

<i>instance ID</i>	Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.
<i>name</i>	(Optional) Enter the name of VXLAN logical network with a maximum length of 30 characters.
<i>vnidVNID</i>	(Optional) Enter the keyword <code>vnid</code> and then enter the ID of the VXLAN. The range is from 1 to 16777215.

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
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S6000.

Example

```
Dell# show vxlan vxlan-instance <1> unicast-mac-remote
Total Local Mac Count:    1
VNI          MAC          TUNNEL
4656         00:00:01:00:00:01    36.1.1.1
```

Related Commands [vxlan-instance](#)- Enable VXLAN Instance configuration on the platform.

show vxlan vxlan-instance unicast-mac-local

Displays the information of the local unicast MAC associated with the logical network related to Network Virtualization Overlay (NVO) Gateway.

Syntax `show vxlan vxlan-instance instance ID unicast-mac-local [logical-network name | vniid VNID]`

Parameters

<i>instance ID</i>	Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.
<i>name</i>	(Optional) Enter the name of VXLAN logical network with a maximum length of 30 characters.
<i>vniid VNID</i>	(Optional) Enter the keyword <i>vniid</i> and enter the ID of the VXLAN. The range is from 1 to 16777215.

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
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S6000.

Example

```
Dell# show vxlan vxlan-instance <1> unicast-mac-local
Total Local Mac Count:    5
VNI          MAC          PORT          VLAN
4656         00:00:02:00:03:00    Te 1/17/1    0
4656         00:00:02:00:03:01    Te 1/17/1    0
4656         00:00:02:00:03:02    Te 1/17/1    0
```



4656	00:00:02:00:03:03	Te 1/17/1	0
4656	00:00:02:00:03:04	Te 1/17/1	0

Related Commands [vxlan-instance](#)- Enable VXLAN Instance configuration on the platform.

show vxlan vxlan-instance statistics interface

Displays the port VLAN statistics information related to Network Virtualization Overlay (NVO) Gateway.

Syntax `show vxlan vxlan-instance instance ID statistics interface interface`

Parameters

<i>instance ID</i>	Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.
<i>interface</i>	Enter the following keywords and slot/port or number information: - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information and then followed by the Vlan ID. The Vlan ID ranges from 0 to 4095. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port information, and then followed by the Vlan ID. The Vlan ID ranges from 0 to 4094. - For a Port Channel, enter the keywords <code>port-channel</code>.

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*.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4(0.0)	Introduced on the S6000.

Example

```
Dell#show vxlan vxlan-instance 1 statistics interface fortyGigE 1/4 100
Port : Fo 1/4 Vlan : 100
Rx Packets : 13
Rx Bytes : 1317
Tx Packets : 13
Tx Bytes : 1321
```

Related Commands [vxlan-instance](#)- Enable VXLAN Instance configuration on the platform.



show vxlan vxlan-instance physical-locator

Displays physical locators related to Network Virtualization Overlay (NVO) Gateway.

Syntax `show vxlan vxlan-instance instance ID physical-locator vtep-ip A.B.C.D`

Parameters

<i>instance ID</i>	Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.
<i>A.B.C.D</i>	Enter the IP address of the VTEP.

Defaults Disabled

Command Modes VXLAN INSTANCE

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
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S6000.

Example

```
Dell#show vxlan vxlan-instance 1 physical-locator
Instance : 1
Tunnel   : count 1
          36.1.1.1 : vxlan_over_ipv4 (up)
```

Related Commands [vxlan-instance](#) — Enable VXLAN Instance configuration on the platform.

show vxlan vxlan-instance logical network

Displays logical network information related to Network Virtualization Overlay (NVO) Gateway.

Syntax `show vxlan vxlan-instance instance ID logical-network [name name]`

Parameters

<i>instance ID</i>	Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.
<i>name name</i>	(OPTIONAL) Enter the keyword <i>name</i> and enter the name of VXLAN logical network up to a length of maximum 30 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*.

Version	Description
9.7(0.0)	Introduced on the S6000-ON.



Version	Description
94.(0.0)	Introduced on the S6000.

Example

```
Dell#show vxlan vxlan-instance 1 logical-network
Instance      : 1
Total LN count : 1
  Name
  bffc3be0-13e6-4745-9f6b-0bcb5877f01      4656      VNID

Dell#$n-instance 1 logical-network n 2a8d5d19-8845-4365-ad04-243f0b6df252
Name : 2a8d5d19-8845-4365-ad04-243f0b6df252
Description :
Tunnel Key : 2
VFI : 28674
Unknown Multicast MAC Tunnels:
  192.168.122.133 : vxlan_over_ipv4 (up)
Port Vlan Bindings:
  Te 1/8: VLAN: 0 (0x80000001),
  Fo 1/12: VLAN: 0 (0x80000004),
```

Related Commands [vxlan-instance](#) — Enable VXLAN Instance configuration on the platform.

clear vxlan vxlan-instance statistics

Syntax `clear vxlan vxlan-instance instance ID statistics`

Parameters

<i>instance ID</i>	Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.

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*

Version	Description
97.(0.0)	Introduced on the S6000-ON.
94.(0.0)	Introduced on the S6000.

clear mac-address-table dynamic all

Clear the MAC address table of all MAC address learned dynamically. It clears both MAC address of the VXLAN and legacy VLAN.

Syntax `clear mac-address-table dynamic all`

Parameters

<i>instance ID</i>	Enter the VXLAN instance ID. The platform supports only the instance ID 1 in the initial release.

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*

Version	Description
9.7(0.0)	Introduced on the S6000-ON.
9.4.(0.0)	Introduced on the S6000.



Virtual Router Redundancy Protocol (VRRP)

Virtual router redundancy protocol (VRRP) is supported by the Dell Networking operating system on Dell Networking OS.

IPv4 VRRP Commands

The following are IPv4 VRRP commands.

advertise-interval

Set the time interval between VRRP advertisements.

Syntax	<code>advertise-interval {seconds centisecs centisecs }</code>	
	To return to the default settings, use the <code>no advertise-interval</code> 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 <code>centisecs</code> 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 <i>Dell Networking OS Command Line Reference Guide</i> .	

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(0.0)	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 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.

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 <code>simple</code> 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
9.7(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.
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.

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 <code>ipv6</code> to clear counters from the IPv6 VRRP group.
	vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> 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, refer to the relevant *Dell 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.
9.4.(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.

debug vrrp

Allows you to enable debugging of VRRP.

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 <code>port-channel</code> then the number. The range is from 1 to 128. - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. - For a VLAN interface, enter the keyword <code>vlan</code> 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 <code>all</code> to enable debugging of all VRRP groups.
bfd	Enter the keyword <code>bfd</code> to enable debugging of VRRP BFD interactions.
database	Enter the keyword <code>database</code> to enable debugging of configuration changes.
interface	Enter the keyword <code>interface</code> to enable debugging of interface state changes..
ipv6	Enter the keyword <code>ipv6</code> to enable debugging for IPv6.
packets	Enter the keyword <code>packets</code> to enable debugging of VRRP control packets.
state	Enter the keyword <code>state</code> to enable debugging of VRRP state changes.
timer	Enter the keyword <code>timer</code> 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
9.7(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.
7.5.1.0	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.

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
9.7(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.
6.2.1.1	Introduced on the E-Series.

disable

Disable a VRRP group.

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
9.7(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.
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.

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 <code>centisecs</code> then the number of <i>centisecs</i> 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
9.7(0.0)	Introduced on the S6000-ON.
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.

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
9.7(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.
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.

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
9.7(0.0)	Introduced on the S6000-ON.
9.0.2.0	Introduced on the S6000.
8.3.16.0	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 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.

Syntax `show config [verbose]`

Parameters

verbose	(OPTIONAL) Enter the keyword <code>verbose</code> 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
9.7(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.
6.2.1.1	Introduced on the E-Series.

Example

```
Dell(conf-if-vrid-4)#show config
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`.

Syntax `show vrrp [vrrp-id] [vrf vrf-name] [interface] [brief] [ipv6]`

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.
vrf vrf-name	(OPTIONAL) Enter the keyword <code>vrf</code> and then the name of the VRF to view active VRRP groups corresponding to that VRF.
interface	(OPTIONAL) Enter the following keywords and slot/port[/subport] 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/subport 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 `ipv6` to view only VRRP IPv6 groups.

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
9.7(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.

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 <code>track</code> 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. • <code>Y</code> = Preempt is enabled. • <code>N</code> = Preempt is not enabled.
State	Displays the operational state of the interface by using one of the following:



Item	Description
	• 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.

Example (Brief)

```
Dell>Interface Grp Pri Pre State Master addr Virtual addr(s)
Description-----
Te 1/3/1 1 100 Y Master 200.200.200.200 200.200.200.201
Te 1/3/1 2 100 Y Master 200.200.200.200 200.200.200.202 200.200.200.203
Description
Te 1/3/1 3 100 Y Master 1.1.1.1 1.1.1.2
Te 1/3/1 4 100 Y Master 200.200.200.200 200.200.200.206
200.200.200.207 ... short desc
Te 1/3/1 254 254 Y Master 200.200.200.200 200.200.200.204 200.200.200.205
Dell>
```

Usage Information

The following describes the `show vrrp` command shown in the following example.

Item	Description
TenGigabitEthernet 1/3...	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.
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.



Item	Description
Tracking states..	This line is displayed if the <code>track</code> 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 1/1/3, 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 1/1/4 priority-cost 10
-----
TenGigabitEthernet 1/4/1, 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 2/1/1 priority-cost 10
    Up TenGigabitEthernet 1/1/4 priority-cost 10
Dell>
```

track

Monitor an interface and lower the priority value of the VRRP group on that interface if it is disabled.

Syntax `track interface [priority-cost cost]`
 To disable monitoring, use the `no track interface` command.

Parameters

<i>interface</i>	(OPTIONAL) Enter the following keywords and slot/port[/subport] or number information: • For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. • For a Loopback interface, enter the keyword <code>loopback</code> then a number from 0 to 16383. • For Port Channel interface types, enter the keywords <code>port-channel</code> then a number. • For a 40-Gigabit Ethernet interface, enter the keyword <code>fortyGigE</code> then the slot/port information. • For a VLAN interface, enter the keyword <code>vlan</code> followed by the VLAN ID. The VLAN ID range is from 1 to 4094.



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
9.7(0.0)	Introduced on the S6000-ON.
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.

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.

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
9.7(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.



Version	Description
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.

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
9.7(0.0)	Introduced on the S6000-ON.
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 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.

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
9.7(0.0)	Introduced on the S6000-ON.
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 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 12 VRRP groups per interface.

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, refer to the relevant *Dell 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.
9.0.2.0	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 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.

version

Set VRRP protocol version for IPv4 group.

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, <i>Virtual Router Redundancy Protocol</i> .
	3	Enter the 2 parameter to specify VRRP version 3 as defined in RFC 5798, <i>Virtual Router Redundancy</i> .
	both	Enter the <code>both</code> 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, refer to the relevant *Dell 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(0.0)	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-1/1/1-vrid-100)#version ?
2                               VRRPv2
3                               VRRPv3
both                            Interoperable, send VRRPv3 receive
both
```

```
Dell(conf-if-te-1/1/1-vrid-100)#version 3
```

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](#)
- [description](#)
- [disable](#)
- [hold-time](#)
- [preempt](#)
- [priority](#)
- [show config](#)
- [virtual-address](#)

clear counters vrrp ipv6

Clear the counters recorded for IPv6 VRRP groups.

Syntax `clear counters vrrp ipv6 [vrid | vrf vrf-name]`

Parameters

vrid	(OPTIONAL) Enter the number of an IPv6 VRRP group. The range is from 1 to 255.
vrf vrf-name	(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
9.7(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.

debug vrrp ipv6

Allows you to enable debugging of VRRP.

Syntax `debug vrrp ipv6 interface [vrid] {all | packets | state | timer}`

Parameters

interface	Enter the following keywords and slot/port[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a Port Channel interface, enter the keywords <code>port-channel</code> then a number. - For a VLAN interface, enter the keyword <code>vlan</code> 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 <code>all</code> to enable debugging of all VRRP groups.
bfd	Enter the keyword <code>bfd</code> to enable debugging of all VRRP BFD interactions.
database	Enter the keyword <code>database</code> to display changes related to group, prefix, and interface entries in the VRRP table.
packets	Enter the keyword <code>packets</code> to enable debugging of VRRP control packets.
state	Enter the keyword <code>state</code> to enable debugging of VRRP state changes.
timer	Enter the keyword <code>timer</code> 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
9.7(0.0)	Introduced on the S6000-ON.
8.3.19.0	Introduced on the S4820T.



Version	Description
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`.

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[/subport] or number information: - For a 10-Gigabit Ethernet interface, enter the keyword <code>TenGigabitEthernet</code> then the slot/port/subport information. - For a port channel interface, enter the keywords <code>port-channel</code> then a number. - For a VLAN interface, enter the keyword <code>vlan</code> then a number from 1 to 4094.
brief	(OPTIONAL) Enter the keyword <code>brief</code> to view a table of information on the VRRP groups.
vrf vrf-name	Enter the keyword <code>vrf</code> 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, refer to the relevant *Dell 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)	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.
8.3.10.0	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[/subport] or object number, description, and time since the last change in the state of the tracked object. • Cost to be subtracted from the VRRP group priority if the state of the tracked interface/object goes DOWN.

Example

```

Dell#show vrrp ipv6
-----
TenGigabitEthernet 5/6/1, 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.

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, refer to the relevant *Dell 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.
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.

- When VRF microcode is not loaded in CAM, the VRID for a VRRP group is the same as the VRID number configured with the `vrrp-group` or `vrrp-ipv6-group` command.
- When VRF microcode is loaded in CAM, the VRID for a VRRP group is equal to 16 times the `vrrp-group` or `vrrp-ipv6-group vrid` number plus the `ip vrf vrf-id` number. For example, if VRF microcode is loaded and VRRP group 10 is configured in VRF 2, the VRID used for the VRRP group is $(16 \times 10) + 2$, or 162. This VRID value is used in the lowest byte of the virtual MAC address of the VRRP group and is also used for VRF routing.

 **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.